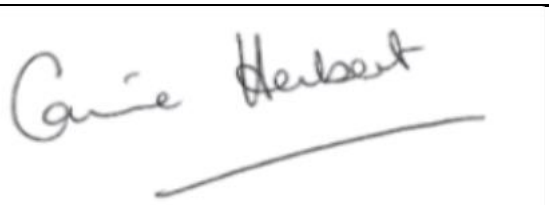
Policy document control box	
Policy title	**Red Balloon Educational Trust** **Online Safety Policy**
Policy owner (including job title)	Maddy Fretwell Head of Data, Systems and Infrastructure, Data Protection Officer, Safeguarding Lead
Version	1.00
Red Balloon approving body	Red Balloon Educational Trust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

Important contacts		
Role	Name	Contact details
Centre Designated Safeguarding Leads (DSLs)	Air - Hannah Curry Worthing - Kim Anderson Norfolk – Louise Fisher Aylesbury - Claire Cockcroft	Hannah.curry@rbair.org.uk Kim.anderson@rbet.ac Louise.fisher@rbet.ac Claire.cockcroft@rbet.ac
RBET Safeguarding Lead	Maddy Fretwell	Maddy.fretwell@rbet.ac

Policy Contents

1. Purpose

Red Balloon Educational Trust comprises four Centres: Red Balloon of the Air (RBAir), RBET-Worthing, RBET- Norfolk and RBET- Aylesbury. Each Centre offers special educational provision to young people unable to access mainstream education. Due to the nature of RBET provision and cohort, online safety is of paramount importance and is therefore considered during all developmental work.

RBAir, in particular, offers a hybrid of online and face-to-face support to students. We are therefore committed to ensuring the safety and wellbeing of students in both the physical and digital worlds, utilising technology to ensure a high quality of support is available for them and embracing new developments to offer them enhanced learning opportunities.

Whilst RBAir's provision makes use of the digital world more prominently than other RBET Centres, whose provision is not hybrid, this policy encompasses all under the RBET umbrella to ensure consistency and protection for all beyond the physical environment. We are determined to ensure that all RBET students and staff remain safe in all online environments. Therefore RBET aims to:

- have robust processes in place to ensure the online safety of students, staff, volunteers and trustees;
- identify and support students that are potentially at greater risk of harm online than others;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole of the RBET community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones');
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The Four Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- As of KCSIE 2025, "content" also includes misinformation, disinformation (fake news), and conspiracy theories, reflecting these new threats in digital environments.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice on:

- Teaching online safety
- Preventing and tackling bullying
- Relationships and sex education
- Searching, screening and confiscation

It also refers to DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including, but not limited to, the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum, in particular the computing programmes of study and PSHE.

RBET is aware of the rapidly developing digital world, particularly the concerns surrounding AI. This policy is therefore written with consideration of DfE expectations as outlined here: Generative AI: product safety expectations - GOV.UK and as discussed in Keeping Children Safe in Education.

3. Roles and responsibilities

Red Balloon Educational Trust (RBET) Trustees

RBET Trustees have overall responsibility for monitoring this policy and holding the Head of Centre to account for its implementation.

RBET Trustees will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure that staff understand their expectations, roles and responsibilities around filtering and monitoring.

RBET Trustees must ensure that RBET has appropriate filtering and monitoring systems in place on all RBET devices and networks.

All Trustees will:

- ensure they have read and understand this policy and the Staff ICT Acceptable Use Agreement;
- ensure that online safety is a running and interrelated theme while devising and implementing any approaches to safeguarding and related policies and/or procedures;
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children and young people in all situations, and a more personalised or contextualised approach may often be more suitable.

RBET Safeguarding Lead

The Safeguarding Lead will maintain an oversight of safeguarding across RBET, including responsibility for best practices and policy compliance. The Safeguarding Lead will ensure that the safeguarding of students and staff remains at the forefront of RBET's practices, by working collaboratively with DSLs and the safeguarding team members to uphold safeguarding standards and meet obligations effectively and providing support where required.

The RBET Safeguarding Lead will collaborate with the central team and each Centre's Head of Centre and members of the safeguarding teams to:

- ensure that this policy is updated in alignment with national legislation and the RBET Cyber Security Policy;
- ensure software and data are managed accurately and effectively to ensure robust procedures are in place to support safeguarding practices;

- ensuring Smoothwall and Cyber Essentials are monitored and maintained, in collaboration with the external IT Provider;
- communicate with and report to the Safeguarding Trustee with relevant safeguarding statistics and information to maintain oversight of all provision under the Trust.

The Head of Centre

At each RBET Centre, the Head of Centre is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout their Centre.

The Head of Centre will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Head of Centre, in collaboration with the RBET Safeguarding Lead and Online Safety Lead, will remain up to date with DfE filtering and monitoring standards, and discuss with the external IT provider what needs to be done to support RBET in meeting the standards, which include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- reviewing filtering and monitoring provisions at least annually;
- blocking harmful and inappropriate content without unreasonably impacting teaching and learning.

The Designated Safeguarding Lead (DSL) and Deputies (DDSLs)

Details about each Centre's DSL and DDSLs are set out in our Safeguarding and Child Protection Policy, as well as in relevant job descriptions. Specific members of the Safeguarding Team are also nominated as Online Safety Lead and Prevent Lead, whose specific responsibilities are outlined below. Please refer to the Important Contacts for specific contact information.

The DSL/DDSLs are ultimately responsible for ensuring online safety within their Centre, in particular by:

- supporting the Head of Centre in ensuring that staff understand this policy and that it is being implemented consistently;
- working with the Head of Centre and RBET Trustees to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;
- leading on understanding and actively monitoring the filtering and monitoring systems and processes in place on all RBET devices and networks, including staff and community training

and support. All online safety concerns received via Smoothwall are reviewed weekly at the safeguarding team meeting;

- working with the Online Safety Lead and external IT provider to make sure the appropriate systems and processes are in place;
- working with the Head of Centre, Online Safety Lead, external IT provider and other staff, as necessary, to address any online safety issues or incidents;
- ensuring that any online safety incidents are logged and managed in alignment with the RBET Safeguarding Policy and each Centre's Safeguarding Procedure and practices and dealt with in line with this policy, including regular reporting to the Head of Centre;
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide staff with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The DDSL Online Safety Lead

The Online Safety Lead is responsible for:

- maintaining and monitoring (in collaboration with the RBET Safeguarding Lead, DSL and the Prevent Lead) appropriate online filtering and monitoring systems, alongside internal monitoring processes including termly stress testing using a dummy student account;
- undertaking (in collaboration with the RBET Safeguarding Lead and RBET Data Protection Officer) relevant risk assessments and data protection impact assessments for all software and tools used across the organisation (these are reviewed regularly);
- coordinating with the RBET Safeguarding Lead and Centre Prevent Lead to deliver staff training on online safety, including all systems and processes such as Smoothwall, ensuring that the Prevent strategy is seamlessly integrated with all online safety training and initiatives;
- maintaining a reporting schedule to support the DSL and Head of Centre with data-led decision making;

The DDSL Prevent Lead

The Prevent Lead is responsible for:

- ensuring that all staff receive appropriate Prevent training regularly, including during any new staff induction, to understand the risks of radicalisation and how to respond effectively;

- engaging with the Local Authority's risk assessment to determine the potential risk of individuals being drawn into terrorism in the local area, considering both online and offline radicalisation risks;
- ensuring the Prevent duty is incorporated into existing Centre and Trust wide policies, such as safeguarding and online safety policies;
- making sure that RBET is a safe space for students to discuss sensitive topics, including terrorism and extremism, and to learn how to challenge extremist ideas;
- understanding the legal basis for sharing personal information about students at risk of radicalisation without consent when necessary, and ensuring compliance with data protection laws;
- collaborating with external agencies, parents[1] to address and mitigate risks of radicalisation;
- undertaking more in-depth training to support RBET's Prevent duty, including information about extremist and terrorist ideologies, making referrals, and working with Channel panels;
- ensuring, in collaboration with the Centre Online Safety Lead, that appropriate online filtering and monitoring systems are functioning effectively to protect students from harmful online content relevant to Prevent;
- following the Centre's safeguarding procedures, including supporting colleagues to report concerns about radicalisation and deciding which agency to refer to, such as the Local Authority, police, social services, or Channel.

The robust structure of each Centre's Safeguarding Team ensures that there is always a member of staff available to receive concerns from staff, parents or students, with the Online Safety Lead maintaining oversight of all concerns logged in CPOMS and Smoothwall during working hours.

The External IT Provider

The external IT provider, in collaboration with the Head of Centre, is responsible for:

- putting in place an appropriate level of security protection, including Smoothwall Filter and Monitor, and ensuring they are installed on all RBET devices. All protection measures are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online during their time with RBET, including terrorist and extremist material;

[1] Wherever the term "parent" is used in the policy, it means any person with parental responsibility for the young person.

- ensuring that RBET ICT systems are compliant with the RBET Cyber Security Policy, secure and protected against viruses and malware, including configuration to prevent the download of unsafe files, and that such safety mechanisms are updated regularly;
- maintaining full security and monitoring of RBET ICT systems, as per contractual obligations;
- maintaining Microsoft Defender, an AI-powered device security solution installed on all RBET devices designed to protect devices from ransomware, malware, phishing and other cyberthreats;
- ensuring RBET remain compliant with Cyber Essentials accreditation, applying annually for certification renewal.

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, including contractors and volunteers, are responsible for:

- understanding, implementing and adhering to this policy and the RBET Staff ICT Acceptable Use Policy;
- knowing that the DSL, Safeguarding Team and IT provider are responsible for the filtering and monitoring systems and processes and ensuring any failings of these systems are reported to the relevant Centre's safeguarding team immediately;
- working with the DSL to ensure that any online safety or cyber bullying incidents are logged in alignment with the Centre's Safeguarding Policy and procedures, and dealt with appropriately in line with this policy;
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here';
- Ensuring all internet use is planned carefully to ensure that it is age-appropriate and supports the learning objects for the specific curriculum or wider research area.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- notify a member of staff or the Head of Centre of any concerns or queries regarding this policy;
- ensure that they and their child have read, understood and agreed to the Learner ICT Acceptable Use Agreement provided during admission.

Although we strive to protect students to the best of our ability, there are limitations to RBET's reach: for example, we cannot monitor non-RBET devices. Therefore parent engagement is critical. Parents are responsible for monitoring their child's social media and safe internet use. For additional information regarding how RBET Centres internally monitor online safety, please see Appendix 3.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Learner
- Hot topics – Childnet
- Parent resource sheet – Childnet

4. Educating students about online safety

All RBET Centres

RBET is aware that our students will not only be working online within the physical Centres, but also outside of the Centre - at their home for example, and that this will not always be via an RBET device covered by our protection. It is therefore imperative that both students and their parents are educated about both the limitations of RBET's reach and the risks involved with using the internet. RBET aims to provide guidance on a range of strategies which staff, students and parents feel confident to use in acting online and know what to do if they see, hear or read anything that makes them feel uncomfortable.

Throughout their time with RBET, students will be taught to:

- understand how to use technology safely, respectfully, responsibly, and securely. This includes protecting their online identity and privacy and keeping up to date with constant changes and developments in technology;
- recognise inappropriate content, contact and conduct, and know how to report concerns both internally to RBET and externally, to the police for example, when required;
- Evaluate how to evaluate online content, for example by cross-checking information before accepting face value, with particular focus on the risks of AI and deepfakes.

By the **end of their time with RBET**, students should know:

- their rights, responsibilities and opportunities, including that the same expectations of behaviour apply in all contexts, including online;

- about online risks, including that any material someone provides to another has the potential to be shared online, and the difficulty of removing potentially compromising material placed online;
- not to provide material to others that they would not want shared further and not to share personal material that is sent to them;
- what to do and where to get support to report material or manage issues online, both internally and externally;
- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and can negatively affect how they behave towards sexual partners;
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail;
- how information and data are generated, collected, shared and used online;
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;
- how to actively communicate and recognise consent from themselves and others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online);

The PSHE curriculum includes discussion of digital resilience, safe socialisation both in person and online and much more. Additionally, online safety principles, including consideration of AI, are embedded throughout the curriculum, where relevant, with adaptations to meet the needs of students with SEND. Students will be taught about online safety as part of the curriculum, as outlined by the National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education.

RBAir Online Safety Induction

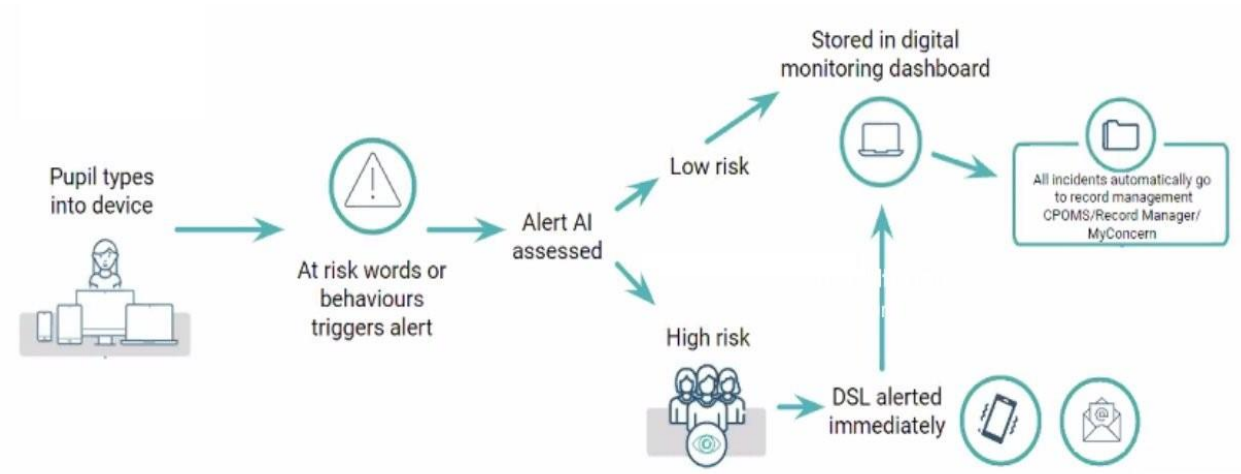
Due to the increased access to the online world and nature of provision at RBAir, all RBAir students complete a mandatory six-week induction programme specifically regarding ‘online safety’; for those of statutory school age, this leads into joining a PSHE group. The Online Safety programme content includes considerations of AI, human rights, scams and gambling, fake news and much more. For RBAir specifically, the PSHE programme is accompanied by the Online Community and Step4Ward programmes to ensure full coverage of complex online safety issues.

5. Educating parents about online safety

RBET will raise parents' awareness of online safety in letters and in information via our website. This policy will be signposted to them during the admissions process and will be accessible via our website.

During admission, parents are informed that all RBET devices have Smoothwall Monitor and Filter installed to ensure robust protection for students, and parent roles and responsibilities are outlined. Below is a summary of Smoothwall Monitor and Filter, as well as a graphic demonstrating Smoothwall Monitor.

- **What is Smoothwall Monitor?** Smoothwall Monitor is a human moderated digital monitoring solution. If any unusual digital behaviours, which signal a child or young person is at risk are detected, an alert is sent to the Centre's Safeguarding Team and logged automatically in our safeguarding software, CPOMS.
- **What is Smoothwall Filter?** Smoothwall's Filter assesses the permissibility of every web page by using AI to evaluate the content, context and construction of the site, and then blocks any harmful content the second it goes live.



If parents have any queries or concerns in relation to online safety, or this policy, these should be raised in the first instance with the Head of Centre or a member of the Safeguarding Team or both. For specific details regarding each Centre's internal monitoring of Smoothwall please see Appendix 3.

The RBET Safeguarding Lead works closely with the Fundraising, Marketing and Communications Team, Heads of Centre and DSLs to ensure communication with all parents regarding online safety, in particular sharing up to date information within the rapidly changing world with regard to AI and social media as and when appropriate. In order to ensure students are protected to the best of RBET's ability the education of, and communication with, parents is of the upmost importance.

6. Cyber-bullying

Definition

Cyber-bullying takes place online, through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the intentional harming of one person or group by another person or group where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that our students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that they know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

RBET will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take, and what the consequences may be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying and online safety. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, trustees and volunteers receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see Section 11 for more detail).

In relation to a specific incident of cyber-bullying, each Centre will follow the processes set out in the Centre-specific Behaviour for Learning Policy. Where illegal, inappropriate or harmful material has been spread among students, all reasonable endeavours will be used to ensure the incident is contained.

If the DSL has reasonable grounds to suspect that possessing such material is illegal, they will report the incident and provide the relevant material to the police as soon as is reasonably practicable.

Examining electronic devices

Authorised staff members (the Head of Centre, members of the Safeguarding Team or an individual approved by the Head of Centre) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting poses a risk to staff or students, or is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- assess the urgency of the search and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Head of Centre or a DSL/DDSL;
- explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- seek the student's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase (see below), any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to cause harm, or undermine the safe environment of the Centre or disrupt teaching, or commit an offence.

If inappropriate material is found on the device, it is up to the DSL and Head of Centre to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if they reasonably suspect that its continued existence is likely to cause harm to any person, or the student or parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **not** view the image.
- confiscate the device and report the incident to the DSL (or DDSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through RBET's complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents may be familiar with generative chatbots such as ChatGPT and Google Bard.

RBET recognises that AI may help support students' learning but may also have the potential to be used to bully or negatively affect others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

RBET will treat any use of AI to bully or negatively affect learners or other members of the RBET community in line with each Centre's Anti-bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment in collaboration with the Online Safety Lead where new AI tools are being used by RBET staff, volunteers or students.

RBET recognises that AI is rapidly evolving and therefore ongoing staff training is required to ensure all individuals are kept up to date with the technology and any relevant legislation surrounding it. The RBET Safeguarding Lead will ensure that legislative changes are communicated with the Head of Centre and DSL, to be disseminated to all staff.

AI is incorporated into all relevant policies, including the Examinations Policy and Curriculum Policy. As and when required, the information regarding AI in any policies will be updated to ensure RBET remains up to date with global and national developments in technology.

7. Acceptable use of the internet in Centre

All students, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the Centre's ICT systems and the internet (see Staff ICT Acceptable Use Policy or Appendix 1 and 2). RBAir has a separate learner ICT Acceptable Use Agreement due to the nature of provision (see appendix 1), However all other RBET Centres apply one agreement as shown in Appendix 2. Visitors will be expected to read and agree to the Centre's terms on acceptable use, if relevant.

Use of the Centre's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through a filtering system. For additional information regarding RBET's monitoring of filtering please see Section 5 or Appendix 3.

8. Students using mobile devices in a Centre

Students may bring mobile devices into their Centre, but are not permitted to use them during:

- sessions;
- clubs or any other activities organised by RBET.

Any use of mobile devices in Centre by students must be in line with the Learner ICT Acceptable Use Agreement (see Appendix 1 and Appendix 2).

Any breach of the Learner ICT Acceptable Use Agreement by a student may trigger disciplinary action in line with each Centre's Behaviour for Learning Policy, which may result in the confiscation of their device.

9. Using RBET devices outside a Centre

Both staff and students may commonly use their devices outside of the Centre; therefore, all users will take appropriate steps to ensure their devices remain secure in all environments and adhere to the Centre's Learner ICT Acceptable Use Agreement, RBET Cyber Security Policy and RBET Staff ICT Acceptable Use Policy. This includes, but is not limited to:

- keeping the device password-protected in combination with Multi Factor Authentication;
- making sure the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- keeping operating systems up to date by always installing the latest updates.

If staff have any concerns over the security of their device, they must seek advice from the Head of Centre and the external IT provider.

10. How RBET will respond to issues of misuse

Where a student misuses any RBET devices, software or internet connections, we will follow the procedures set out in our relevant policies, including each Centre's Anti-bullying Policy, Behaviour for Learning Policy, and Learner ICT Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses any RBET systems or devices or does not adhere to the RBET Cyber Security Policy and RBET Staff ICT Acceptable Use Policy, or RBET Bring Your Own Device Policy if applicable, where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

RBET will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber security, cyber-bullying and the risks of online radicalisation.

All staff members will receive online safety refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, and staff meetings) to update their knowledge and skills.

By way of this training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse. Staff will also be made aware that children can abuse their peers online through:

- abusive, threatening, harassing and misogynistic messages;
- non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
- sharing of abusive images and pornography, to those who don't want to receive such content;
- physical abuse, sexual violence and initiation/hazing type violence.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse;
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks;
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

All members of each Centre's Safeguarding Team (DSL and deputies) and the RBET Safeguarding Lead will undertake child protection and safeguarding training, which will include online safety, at least every two years. The Online Safety Lead will also attend additional online safety focused training annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

12. Monitoring arrangements

The Safeguarding Team logs behaviour and safeguarding issues related to online safety in the same manner as any other form of safeguarding concern.

This policy will be reviewed every year by the RBET Safeguarding Lead and each RBET Head of Centre, in collaboration with Centre Online Safety Leads. At every review, the policy will be shared with RBET Trustees. The review will be supported by relevant risk assessments considering all software and online platforms used by staff and learners across RBET. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This Online Safety Policy should be read in conjunction with our other relevant policies including:

- Attendance Policy
- Behaviour for Learning Policy
- Child-On-Child Abuse Policy
- Complaints Policy
- RBET Data Protection Policy and privacy notices
- RBET Cyber Security Policy
- RBET Bring Your Own Device Policy
- Safeguarding and Child Protection Policy
- RBET Staff ICT Acceptable Use Policy
- Learner ICT Acceptable Use Agreements (Appendix 1 and Appendix 2)
- Staff disciplinary procedures

Appendix 1: RBAir Learner ICT Acceptable Use Agreement

For information

Students at Red Balloon of the Air (RBAir) access sessions from home; for this reason, we have a filtering and monitoring system in place. Learners should therefore be aware that all communications through the ICT system, including RBAir email addresses and Microsoft Teams, have keystroke monitoring.

RBAir device:

I confirm that I will only access RBAir's ICT systems using my RBAir laptop. I will not log in using any personal device.

LEARNER:

Signed:_____

Print name:_____

Date:_____

.

Acceptable Use:

When I use RBAir's ICT systems (e.g. laptop computer) I will:

- use RBAir ICT equipment with care and report any damage which occurs as soon as possible;
- always use the ICT systems and the internet, including AI tools, responsibly and for educational purposes only;
- behave appropriately and respect the staff and other learners who may be attending;
- keep my username and passwords safe and not share these with others;
- keep my private information safe at all times;
- tell a member of staff or Link Mentor immediately if I find any material that could upset, distress or harm me or others;
- always log off or shut down a computer when I'm finished working on it;
- comply with copyright regulations;
- be transparent when AI tools have been used to assist with assignments or tasks.

I will not:

- access AI tools to create or any inappropriate content including, but not limited to,
    - illegal content
    - discriminatory content (e.g. sexist, racist or homophobic content)
    - sites that promote drugs or substance abuse
    - extremist content (e.g. the promotion of terrorism)
    - gambling sites
    - malware and/or hacking software;
- use my RBAir email to sign up for accounts except those specifically instructed by a staff member, e.g. GCSE Pod;

- attempt to circumvent the content filters or other security measures installed on the ICT systems, and will not try to access parts of the system that I do not have permission to access;
- use any device to make recordings of staff or students;
- use any inappropriate language when communicating online, including in emails;
- behave online in a way which may bring RBAir into disrepute;
- log in to the ICT system using someone else's details;
- arrange to meet anyone offline without first consulting my parent/carer and Link Mentor;
- use AI tools to plagiarise or misrepresent my own work;
- input personal, sensitive or confidential information into AI tools;
- download or install any software or files on RBAir's ICT equipment or open emails or attachments from people that I do not know.

Agreement and Understanding:

LEARNER

By signing this document, I confirm that I have read, understood and will comply with all of the above.

Signed:_____

Print name:_____

Date:_____

PARENT/CARER

I will support my child to abide by this agreement.

Signed:_____

Print name:_____

Date:_____

Appendix 2: RBET Learner ICT Acceptable Use Agreement

The below Learner ICT Acceptable Use Agreement is signed by all students and parents/carers upon admission to RBET-Norfolk, RBET-Worthing and RBET-Aylesbury.

Acceptable use agreement for learners

Acceptable use of the Centre's ICT facilities and internet: agreement for learners and parents/carers

Name of learner:

When I use the Centre's ICT facilities (like computers and equipment) and go on the internet in the centre, I will not:

- Use them without asking a teacher or mentor first, or without a teacher/mentor in the room with me
- Go on any inappropriate websites
- Go on Facebook or other social networking sites
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use unkind or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes, and they must have given permission for me to share their pictures
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the Centre will check the websites I visit and how I use the Centre's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a Centre laptop or online that upsets me, or that I know is unkind or wrong.

I will always be responsible when I use the Centre's ICT systems and internet.

Signed (Learner):	**Date:**

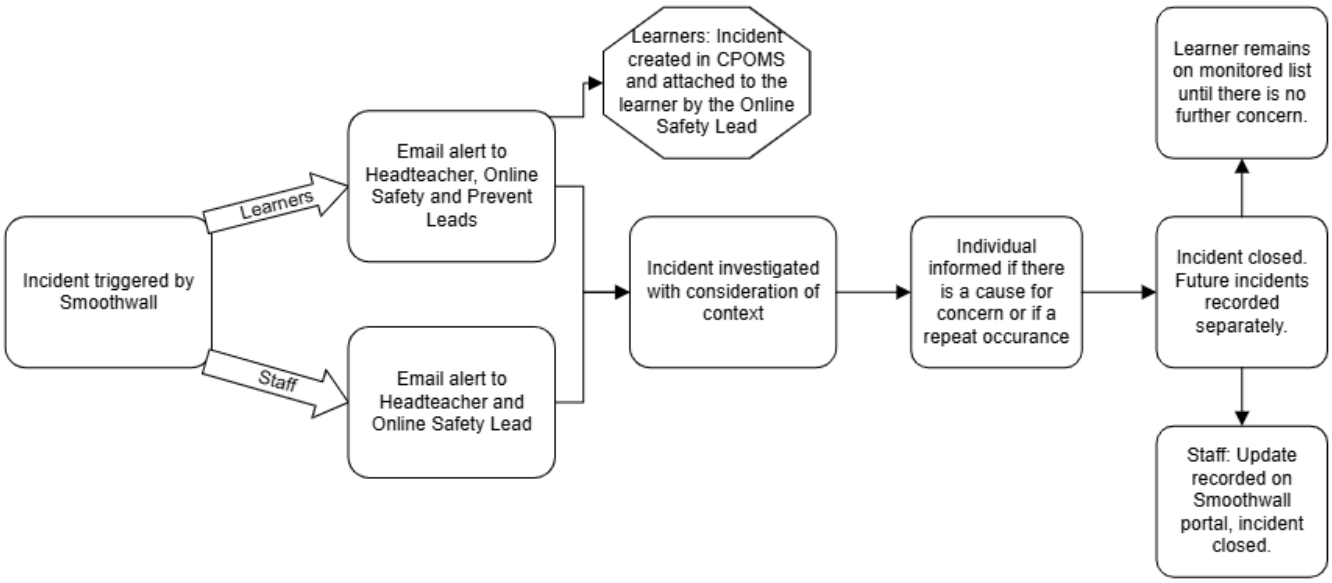
Parent/carer agreement: I agree that my child can use the Centre's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the Centre's ICT systems and internet, and for using personal electronic devices in the Centre, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Smoothwall Monitoring and Filtering

Each Centre's Safeguarding Team includes individuals from across the staff body to ensure a variety of perspectives and maximise the availability of the team to ensure there is always someone whom staff can contact, including a member of the Senior Leadership Team.

- The Safeguarding Team meets regularly to review: open safeguarding incidents; monitored students; Smoothwall alerts within the last seven days; attendance, focusing on those below 70%. For additional information on how attendance is managed at each Centre, please see the relevant Centre's Attendance Policy.
- Smoothwall statistic are reviewed to track progress, patterns and potential areas of development specifically focusing on online safety led by the RBET Safeguarding Lead in collaboration with each Centre's safeguarding team.
- Minutes are taken for all safeguarding team meetings as evidence of monitoring and for future reference where required.



Internal management of Smoothwall Monitor and Filter:

RBET actively monitors online safety incidents via Smoothwall's portal and email alerts. A minimum of two members of the Safeguarding Team receive email alerts for all Smoothwall Monitor and Filter concerns for students, to ensure full coverage throughout the working week. Smoothwall concerns above the set threshold are then automatically integrated within CPOMS to be attached to a student profile and allocated to the most relevant member of the Safeguarding Team by the Online Safety Lead or other member of the safeguarding team, coordinating and aligning the CPOMS and Smoothwall dashboards as part of their role. The infographic above outlines this internal process.

Students will remain on the CPOMS monitored list until deemed appropriate to ensure their understanding of the incident is clear. All concerns relating to a member of staff will be handled under HR procedures following investigation.

Only the RBET Safeguarding Lead and each Centre's DSL receive staff Smoothwall alerts to ensure staff privacy is protected whilst safeguarding best practice is enforced.

Informing Students and Staff of Smoothwall Incidents

When a Smoothwall incident occurs, the Safeguarding Team will only actively inform staff and students of the incident if there is a cause for concern or if it is a repeated occurrence, as we understand that many terms are used in casual conversation which we are not concerned about. Communication with staff and students will be handled by the DSL or DDSL.