The Blue Coat School

ONLINE SAFETY POLICY

Approved by the Governors' Safeguarding, Health and Safety Committee

Signed: _____

(K Gilmore – Chair of Safeguarding, Health and Safety Committee)

Date: _____

This Online Safety Policy was devised by the Director of ICT and the Estates & Compliance Manager in consultation with the Senior Leadership Team and colleagues in the School.

Date of Next Review: Lent 2024

The Blue Coat School Birmingham Limited

ONLINE SAFETY POLICY

1. INTRODUCTION

1.1
The Internet is a valuable resource that can raise educational standards by offering pupils and staff opportunities to search for information from a very wide range of sources around the world. However, some of the information to be found on the Internet is inappropriate to schools and the following policy helps to define appropriate and acceptable use by pupils and staff at the School.

1.2
The implementation of this policy is the responsibility of all members of staff. Mrs Helen Andrews is the named governor for online safety.

1.3
The policy has been drawn up by the Director of ICT after consultation with the Estates and Compliance Manager, Pre-Prep ICT Coordinator and the Senior Leadership Team and has been written with reference to the Think U Know (thinkuknow.co.uk) website and training literature. Further resources are listed in Appendix 1.

1.4
This Policy should be read in conjunction with other whole school policies including those set out in Section 8.1. It should also be read in conjunction with the DfE statutory guidance: 'Keeping Children Safe in Education September 2022' and the DfE non-statutory guidance, 'Teaching Online Safety in School' June 2019.

1.5
The Blue Coat School Online Safety Policy applies to all staff in the School including those in the Early Years Foundation Stage (Nursery and Reception).

1.6
The Blue Coat School Online Safety Policy is available for parents on the School website and in Main Reception and the Pre-Prep Office.

2. ENSURING APPROPRIATE AND SAFE INTERNET ACCESS

2.1
Through active management of hardware, software and the computer network, the School has taken every practical measure to ensure that pupils and staff do not encounter upsetting, offensive or otherwise inappropriate material when they use the Internet in School. The following measures have been put in place:

2.1.1 Internet Security

2.1.1.1
The School Internet Service Provider (ISP) is Virgin Media Business and its service is filtered in two layers: initially by the powerful Cloud Hybrid Smoothwall™, which provides seamless on and offsite filtering, (www.smoothwall.com) and secondly by Google's Cloud based "Safe Search" facility. These together provide high-level intelligent filtering. This enables comprehensive management of web-browsing at a user level and includes detailed, customisable reporting.

2.1.2 E-Mail Security

2.1.2.1
The School uses the cloud-based Google Workspace (formerly G Suite) service as its E-Mail provider which gives users the familiar Gmail interface. Before any E-Mail enters the School's systems it is filtered for spam / phishing by a cloud based third-party service provided by Vipre Mail (www.vipre.com). The Panda Adaptive Defence 360 protection technology is resident on all desktop computer systems and cloud systems in the School and ensures protection against Email-borne threats such as spam, viruses, and phishing. The E-Mail cloud server also uses advanced E-Mail authentication techniques.

2.1.3 Social Networking

2.1.3.1
Social Networking, Blogging and Newsgroups are blocked by the School's filtering systems. Personal use of Facebook and other such sites are explicitly blocked. Some aspects of social media are allowed in order to manage content on the School's Twitter, Instagram and Facebook accounts.

2.1.4 Online Safety Awareness and Training

2.1.4.1
The School facilitates annual presentations on online safety for pupils, staff and parents in order to increase their understanding and awareness of safe internet usage. Staff are trained in safeguarding and child protection, including online safety, initially as part of their induction and at least annually thereafter.

2.1.4.2
Staff recognise that abuse and bullying can take place online and also that technology may be used to facilitate offline abuse. Such abuse may be by an adult, adults or by another child or children. It can include online sexual harassment, which may be stand-alone or be part of a broader pattern of abuse. Staff are also aware that some groups of pupils such as girls and children with SEND are potentially more at risk of abuse. Any such abuse will be dealt with in accordance with the procedures set out in the Safeguarding and Child Protection Policy.

2.1.4.3
When teaching about online safety, staff recognise that there is a possibility that a child (or more than one child) in the lesson may be suffering from online abuse. They therefore ensure that a safe environment is created in which children can raise any concerns. If the teacher is already aware of a child who has been abused or who is being abused or harmed online then advice is sought from a Designated Safeguarding Lead about how best to support the child. If a child makes a disclosure as a result of a lesson on Online Safety, then this will be dealt with in accordance with the procedures set out in the Safeguarding and Child Protection Policy.

2.1.4.4
Where children are engaged in distance learning for reasons such as self-isolation or quarantining, staff will ensure that the online provision is appropriate. Links to any websites and apps referenced during Distance Learning lessons are checked by staff before children are signposted to them.

3. THE INTERNET IN SCHOOL

3.1
The School takes staff and pupils' online safety extremely seriously and has devised a comprehensive plan for safe Internet use:

- Children are taught about safeguarding, including online safety as part of a broad and balanced curriculum.
- Regular online safety awareness sessions are embedded within the Computing scheme of work.
- Pupils will only access the Internet from a School networked computer or tablet in the presence of a teacher. Some pupils have access to a managed Chromebook, which they are permitted to use at home. This is still monitored remotely.
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of the pupils.
- Staff will be particularly vigilant when pupils are undertaking their own searches and will check that the pupils are following the agreed search plan.
- Pupils will be taught to use E-Mail and other Internet services responsibly in order to reduce the risk to themselves and others of exposure to inappropriate material.
- The School's Responsible Computer Use guidelines will be posted near computer systems.
- The Estates and Compliance Manager and Director of ICT will monitor the effectiveness of Internet access policies.
- The Estates and Compliance Manager and Director of ICT will ensure that the Online Safety Policy

is implemented effectively.

- The Estates and Compliance Manager and Director of ICT will ensure that all computer systems are routed through the School's Internet filtering systems.
- The School's methods to minimize the risk of pupils being exposed to inappropriate material will be reviewed frequently.

3.2
The School believes that the measures in place are highly effective. However, due to the linked nature of the Internet, it is not possible to **guarantee** that material of an inappropriate nature will not ever appear on computer screens at the School. The School cannot, therefore, accept liability for the material accessed or any consequences thereof.

3.3
Pupils at the School are taught to tell a teacher **immediately** if they come across any material that makes them feel uncomfortable. If there is an incident in which a pupil views offensive or upsetting material on a School computer, the School will endeavor to respond to the situation quickly and on a number of levels as follows:

- Responsibility for incidents involving pupils will be taken by the Director of ICT, the Estates and Compliance Manager and a Designated Safeguarding Lead (DSL).
- All the teaching staff will be made aware of the incident if appropriate.
- If staff or pupils discover unsuitable websites the Director of ICT and Estates and Compliance Manager will be informed.
- The website(s) in question will be added to a locally maintained list of banned URLs.
- It may be deemed appropriate to report specific websites to the Internet Watch Foundation (www.iwf.org.uk) and / or Child Exploitation and Online Protection Centre (www.ceop.police.uk/Safety-Centre).

3.4
Pupils are expected to play their part in reducing this risk by following the *Rules for Responsible Use of Technology* guidelines. These have been implemented to help protect pupils from exposure to Internet sites carrying offensive material. If unacceptable material is accessed deliberately by a pupil, then the teacher reserves the right to remove the privilege of using the Internet from that child until s/he proves that s/he can be more responsible. Further misuse will result in parents being informed after the Headmaster, the Head of Pre-Prep, and the Head of Prep has been notified.

3.5
The School cannot accept any responsibility for access to the Internet outside School even if pupils are researching a topic related to School.

3.6 The Internet in School - Security of the School ICT Network

3.6.1
The Estates and Compliance Manager will ensure that the security strategies in place on the School's computer network are sufficient to protect the integrity of all networked computers. Access policies will be reviewed regularly and improved as and when necessary.

3.6.2
Because connection to the Internet significantly increases the risk that a computer on a computer network may be infected by viruses, or accessed by unauthorized personnel, the School's anti-virus protection and E-Mail protection are updated automatically and strict user policies are in place.

4. THE INTERNET IN THE CURRICULUM

4.1 PSHE curriculum

4.1.1
Online safety is included in the Relationships strand of the PSHE curriculum. The children are taught how to keep safe online and who to go to for help. They are taught about their online rights and responsibilities; what positive, healthy and respectful online relationships look like; the effects of their online actions on others; and how to recognise and display respectful behavior online.

4.2 Teaching about online safety

4.2.1
Online safety is taught in age and developmentally appropriate ways. It also focuses on the underpinning knowledge and behaviours required for using the online world safely and confidently regardless of the device, platform or app. Underpinning knowledge and behaviours include:

- How to evaluate what is seen online making judgements and not automatically assuming that what is seen is true, valid or acceptable.
- How to recognise techniques used for persuasion and manipulation.
- Acceptable and unacceptable online behavior both from the children themselves and from others and how these standards equate to offline behaviours.
- How to identify online risks and make informed decisions about how to act.
- How and when to seek support, particularly if they are concerned or upset by something they have seen online.

4.3 Using the Internet to Enhance Learning

4.3.1
The Internet is an essential element in a 21st century school environment. The Blue Coat School has a duty to provide pupils with reliable Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be:

- Taught how to use a variety of web browsers.
- Taught what acceptable Internet use means and given clear guidelines for this.
- Educated in the effective use of the Internet for research, including the skills of retrieval and evaluation.
- Shown how to publish and present information to various audiences.
- Taught the importance of considering information before accepting its accuracy.

4.3.2
As in other areas of their work, staff recognise that pupils learn most effectively when they are given clear objectives for Internet use.

4.3.3
Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the Internet may be by teacher demonstration.
- Pupils may be given a suitable web page or a single website to access.
- Pupils may be provided with lists of suitable websites which they may access.

4.3.4
Older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to follow the *Rules for Responsible Use of Technology* guidelines and will be informed that checks can and will be made on files held on the School's computer systems and cloud systems and the sites accessed.

4.3.5
Pupils accessing the Internet will be supervised by a teacher at all times. Pupils in KS2 will only be allowed to use the Internet once they have understood the *Rules for Responsible Use of Technology* guidelines and accepted the need for these rules. It is unrealistic for pupils below KS2 to understand and accept these guidelines and so it is the teacher's responsibility to ensure they are kept safe whilst on-line.

4.4 Using Information from the Internet

4.4.1
In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that most of the information on the Internet is intended for an adult audience, that much of it is not properly audited / edited and that a substantial percentage of it is copyrighted.

4.4.2
Pupils will be taught to expect to find a wide range of content, wider than is found in the School library or on television.

4.4.3
Staff will ensure that their pupils are aware of the need to validate information whenever possible before accepting it as accurate, especially when considering non-moderated information from the Internet.

4.4.4
When copying information from the Internet, pupils and staff will be taught to comply with the laws of copyright, acknowledging authors and publishers when appropriate.

4.4.5
Pupils will be made aware that the author of an E-Mail or web page may not be the person it appears to be.

4.5 Using E-Mail

4.5.1
Pupils will be taught how to use E-Mail applications and the conventions of using E-Mail to communicate with others. It is important that E-Mail communications are properly managed to ensure appropriate educational use, and that the good name of the School is maintained. To that end:

- Pupils will only be allowed to use E-Mail once they have been taught the *Rules for Responsible Computer Use* guidelines and understand these rules.
- Pupils will be given individual addresses with the **thebluecoatschool.com** domain name.
- The sending of E-Mails by pupils will be restricted to internal addresses only – i.e. those with an **@thebluecoatschool.com** address.
- Pupils will be taught how to access their E-Mail accounts in School and under supervision of an adult at home.
- Pupils may have the contents of E-Mail messages they compose checked by members of staff.

4.6 Social Networking and Personal Publishing

4.6.1
The Blue Coat School prevents pupil access to social networking / blogging websites such as Facebook and Twitter as these services usually impose an age restriction on users of 13+ years. Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents are advised that the use of social network spaces outside School brings with it a range of dangers for primary-aged pupils and that they should use extreme care when accessing social networking sites outside School. Social Networking, Blogging and Newsgroups are blocked by the School's filtering systems.

4.7 Video-Conferencing and Webcams

4.7.1
Pupils in Years 5 and 6 are allowed to use the Video-Conferencing and Webcams built in the iMac computers and iPads but only within the confines of the Local Area Network.

4.8 Managing Emerging Technologies

4.8.1
Emerging technologies will be examined for educational benefit and the risks discussed before use is allowed in School. The Senior Leadership Team is aware that technologies such as mobile phones with wireless Internet access can bypass School filtering systems via the mobile data network (3G/4G/5G) and present a new route to undesirable material and communications. Pupils at The Blue Coat School are not permitted to have mobile phones or mobile gaming devices in School. Any unauthorised device which connects to the School's Wi-Fi will be automatically redirected to a logon prompt, blocking access to the Internet until this user has gained permission and credentials to access the Internet from this device. All wireless devices connected to the School's Wi-Fi are monitored.

4.8.2
The School has two grouped sets of pupil iPads (one for Prep and the other for Pre-Prep) which are loaned out for pupil use. The School also has a number of other iPads which are permanently loaned to staff. These are securely managed centrally by the ICT Department and 'apps' are loaded onto the devices once their

educational benefit has been evaluated by the Deputy Head Academic. The iPads share the same stringent Internet filtering as all PCs and Chromebooks in the School. If necessary, iPads and Chromebooks can also have their Internet monitored off-site.

5. PUBLISHING PUPILS' IMAGES AND WORK

5.1
The Pupil Privacy Policy and the School's Terms and Conditions explains the School's intended use of a pupil's images and videos. These documents are provided to parents when a place is offered and inform parents that they also have the right to withdraw consent at any time.

5.2
When the use of personal data becomes more privacy intrusive, such as the use of full names alongside images (e.g. on the School website, social media or in a newsletter), parental consent is sought on an individual basis before the content is published.

6. THE BLUE COAT SCHOOL WEBSITE (thebluecoatschool.com)

6.1
The School website is intended to:

- Provide accurate, up-to-date information about the School.
- Promote the School.
- Celebrate pupils' work and achievements.

6.2
The Director of External Relations is responsible for uploading content to the School website, and for ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

6.3
Current parents are able to access information specific to them via the School portal. Parents are provided with a login as their child enters the School and they are able to set their own password to access future information.

7. REVIEW – MONITORING

7.1
All teachers are responsible for monitoring the use of the Internet within their classrooms and for ensuring that unacceptable material is not accessed.

7.2
The Director of ICT and Estates and Compliance Manager have responsibility for checking that no inappropriate material is on the School system, and the children are made aware that teachers have access to all their folders of work. The Estates and Compliance Manager also ensures that the computer system and cloud systems is regularly checked for computer viruses.

8. RELATED POLICIES, MONITORING AND POLICY REVIEW

8.1
This Policy should be read in conjunction with other related whole school policies including: ICT Acceptable Use; Social Media; Anti-Bullying; Behaviour Management and Exclusions; Safeguarding and Child Protection and PSHE (including Relationships Education) Policy.

8.2
This Online Safety Policy will be presented to the Governors' Safeguarding, Health and Safety Committee for approval annually. The minutes of this meeting will be presented to the Governors.

APPENDIX 1: Useful Resources for Staff

Childnet
childnet.com

Digizen
digizen.org

Cyberbullying
cyberbullying.org

CBBC Stay Safe
bbc.co.uk/cbbc/findoutmore/stay-safe-facts

Child Exploitation and Online Protection Centre
https://www.ceop.police.uk/safety-centre/

Think-U-Know
thinkuknow.co.uk

Family Online Safety Institute
www.fosi.org

Internet Watch Foundation
iwf.org.uk

Karl Hopwood – Online Safety Ltd
www.esafetyltd.co.uk

SKIPS Educational
skipseducational.org/

(Updated list - 09.01.2023)