The Bramptons Primary School

E-Safety Policy

1.0 Introduction

1.1 The school has a duty to safeguard and protect the children at The Bramptons Primary School, including when they use the internet. This means protecting them from maltreatment, preventing impairment of their health and development, enabling them to grow up in a safe and caring environment.

1.2 The internet is also an essential part of 21st century life, particularly in terms of education, business and social interaction. The children of today are growing up in a world where they live their lives seamlessly on and offline. They see no distinction between the two. Although this does present some positive and exciting opportunities, there are also challenges and risks associated with this.

1.3 The school recognises the importance of providing pupils with quality internet access as part of their learning experience. We take a whole school approach to E-safety that is embedded across the school.

1.4 The staff and governors have a responsibility to educate pupils in relation to E-Safety matters, including teaching them the appropriate behaviours and skills to enable them to remain both safe and legal when using the internet and related technologies, both inside and outside of the school environment.

1.5 This policy should be read and implemented in conjunction with the Child Protection and Safeguarding Policy, the Anti-Bullying Policy and the Staff and Volunteers Code of Conduct (including the Acceptable Use Policy and Agreement).

1.6 The school will take all reasonable precautions to ensure that users only access appropriate material on the website. However, due to international scale and the linked nature of internet content, it is not possible to guarantee that unsuitable material will **never** appear on a school computer. The important thing is that the children are given the tools, including building resilience, so they know how to respond appropriately should such an incident occur.

1.7 The school E-Safety Lead and Designated Safeguard Lead is the Head Teacher, Mr John Gillett, and the E-Safety Governor Lead is Chris Clyne.

2.0 The Risks

2.1 We recognise the risks to the children associated with them having access to the internet. There are four potential areas of risk.

- **Content** - Being exposed to illegal, inappropriate or harmful content. For example, pornography, racism, misogyny, self-harm and suicide.

- **Contact** - Being subjected to harmful online interaction with other users, for example child to child abuse, grooming to exploit them for sexual, criminal, financial or other purposes.

- **Conduct** - Online behaviour that increases the likelihood of, or causes, harm, for example sharing, making, sending and receiving explicit images.

- **Commerce** risks including online gambling, inappropriate advertising and financial scams.

2.2 The school understands the importance of teaching children to recognise the risks and how to protect themselves from them.

3.0 Teaching E - Safety

3.1 It is important that the school fosters an open environment in which children and young people are encouraged to ask questions and participate in discussions about the benefits and risks associated with their online life.

3.2 Every opportunity is taken across the curriculum to teach children about staying safe online. It is also specifically included in Relationship, Computing and PHSE lessons.

3.3 Taught in Relationships and PHSE Lessons:

- What positive, healthy and respectful online relationships looks like.
- The effect of our online actions on others.
- How to display acceptable behaviour online.
- How to recognise unacceptable behaviour online.

3.4 Taught through the Computing Curriculum:

- How to use technology safely, responsibly, respectfully and securely.
- Where to go for help and support when they have concerns about content or contact on the internet or other online technology.
- Helping children consider:

    - Whether a website or email address is real or fake.
    - What cookies do and the information being shared.
    - If a person or organisation is who they say they are.
    - Why a person wants them to see, send or believe something.
    - Whether something posted is a fact or someone's opinion.
    - Why a person or organisations wants their personal information.
    - Why age restrictions exist and the dangers of not complying with them.

3.4 In terms of online behaviour, teaching will include:

- That the same standard of behaviour should be displayed online as offline.
- How to recognise unacceptable behaviour in others.
- Why people behave differently online (Anonymity, invisibility)
- What a constructive discussion looks like and how online disagreements can escalate.
- Unacceptable behaviour passed of as banter or joking.

3.5 In relation to how content can be shared, teaching will include:

- What a digital footprint is and how it Is created.
- How a digital footprint can affect future prospects.
- How cookies work.
- What content can be shared, tagged, traced.
- How difficult it is to remove something a user regrets sharing.
- Risk of identity theft,
- What it is illegal to do online.

3.6 In relation to Misinformation, Disinformation, and Hoaxes teaching will include:

- Why individuals or groups share false information to deliberately deceive.
- How false or misleading information can be shared inadvertently.
- How genuine information can be shared deliberately with an intent to cause harm.
- |How to check authenticity online.

3.7 In terms of Password Phishing, teaching will include:

- Why passwords are important and how to keep them safe.
- How to recognise phishing scams and how scammers try to get login credentials and passwords.
- Importance of online security to protect against viruses.
- What to do when a password is compromised.

3.8 In relation to Persuasive Design teaching will include:

- That a majority of games and platforms are businesses designed to make money.
- That many devices, apps and games are designed to keep users online for as long as possible in the hope you will spend money.
- How designers use notifications to encourage users back online.

3.9 In respect of Online Abuse, teaching will include:

Explaining the types of online abuse including sexual, harassment, bullying, trolling and intimidation.

- Explaining when abuse becomes illegal such as hate crime and blackmail.
- How to get help and support if they suffer online abuse.
- How to respond when abuse is anonymous.
- The implications of online abuse.

3.10 In relation to Online Radicalisation, teaching will include:

- How to recognise extremist content.
- Understanding actions that are criminal activity.
- Exploring techniques used for persuasion.
- How to access support from trusted adults.

3.11 In terms of online challenges, teaching will include:

- Explaining what an online challenge is and that some can be harmful or even illegal.
- How to assess if a challenge is safe or potentially harmful.
- Emphasising that it is ok not to take part.
- Where to get help if worried about a challenge.
- Understanding the importance of telling a trusted adult about challenges that involve threat or secrecy.

3.12 In relation to Content that Incites, teaching will include:

- Ensuring children know that online content (sometimes gang related) can glamorise the possession of weapons and drugs
- Explaining that to intentionally encourage or assist an offence is also a criminal offence.
- Ensuring pupils know how and where to get help if worried about involvement in violence

3.13 In relation to Fake Profiles, teaching will include:

- That not everyone online is who they say they are.
- Explaining that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts).
- How to look out for fake profiles, for example, profile pictures that don't like right, accounts with no followers or thousands of followers or a public figure who doesnot have a verified account.

3.14 In relation to Grooming, teaching will include:

- Understanding the different types of grooming and motivations for it, for example radicalisation, child sexual abuse and exploitation, gangs (county lines), financial exploitation (money mules).

- Understanding the boundaries in friendships with peers, families and others.
- The key indicators of grooming behaviour.
- Explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult.
- How and where to report it both in school, for safeguarding and personal support, and to the police.

3.15 In relation to Live Streaming, teaching will include:

- The risks associated with live streaming including the potential for it to be recorded and/or shared.
- That children should not do anything online that they would not do offline.
- The risks of watching videos being live streamed – they do not know what will come next so they may see something that is not age appropriate.
- The risk of grooming.

3.16 In relation to the Impact on Wellbeing and Confidence, teaching will include:

- That online activity can adversely affect their self-image and identity, their online reputation, and their health and wellbeing,
- Most images are not true depictions of people. Image filters and digital enhancement is used.
- Exploring the role of social media influencers, including those that are paid to influence the behaviour of their followers.
- Understanding that “easy money” lifestyles and offers may be too good to be true.
- How photograph manipulation works and why people do it.

3.17 In relation to the impact on Quality of Life, Physical and Mental Health and Relationships, teaching will include:

- Helping children to critically evaluate what they are doing online and why they are doing it. Also, the amount of time they are spending online.
- Encouraging the children to think about quality versus quantity of online activity.
- Encouraging children to think about whether they are actually enjoying the time they are spending online or are they doing it from habit or as a result of peer pressure?
- Helping children understand that the more time they spend online the less time they have to do other activities.
- Exploring the impact of excessive social media activity on anxiety, depression and other mental health issues.
- Explaining the excessive online activity can result in isolation and loneliness and the importance of discussing this with an adult and seeking help.

3.18 All E-Safety teaching is age appropriate and many of the above areas will not be covered at KS1. As the children move up the school the number of areas covered increases.

3.19 We are aware that providing children with the knowledge, may result in them recognising that they are being harmed or abused which could lead to a disclosure. Staff are fully aware of the necessary course of action if a disclosure is made.

3.20 We require the children to sign up to an Acceptable Use Agreement to help them stay safe online at school and at home (Appendix A).

4.0 Vulnerable Children

4.1 All children can be vulnerable online and vulnerability can fluctuate depending on age, developmental stage and personal circumstances.

4.2 Those children with special educational needs and Looked After Children are more susceptible to online harm. They may find it more difficult to recognise when they are at risk from harm or may not have the support from family and friends in staying safe on the internet.

4.2 Staff will ensure that the teaching in relation to online safety will be accessible to all children, at an age appropriate level. This may mean planning differentiated lessons and/or using different resources.

5.0 Monitoring & Filtering

5.1 It is prohibited for children to bring mobile devices into school, therefore the only access they have to the internet during school time is via Chromebooks. Their use of the Chromebooks is closely monitored by two members of Staff.

5.2 We have very effective filtering measures in place and are conscious of the importance of achieving a balance; protecting the children but also ensure they are able to access the information they need. If there are occasions on which staff cannot access a site they need due to filtering, arrangements are in place to enable them to gain access quickly.

5.3 The school receives regular reports that show internet usage across the school.

6.0 Roles and Responsibilities

6.1 Governors

- Approve this policy and review its effectiveness.
- Ensure that the school has effective measures in place to protect children while working remotely. Also that the arrangements are reviewed as necessary.
- Ensure an appropriate senior manager is appointed to the role of DSL.
- Support the school in encouraging parents to become engaged in online safety activities.
- Ensure all staff undergo safeguarding training, including online safety, at induction.
- Ensure the monitoring and filtering systems that are in place are being used effectively.
- Ensure children are taught about online safety as part of a broad and balanced curriculum and that there is a whole-school approach to delivering this teaching.

6.2 Head Teacher/DSL

At The Bramptons the Head Teacher is the DSL and the Lead for E-Safety. His responsibilities include:

- Fostering a culture for safeguarding where online safety in fully-integrated into whole-school safeguarding.
- Taking day-to-day responsibility for online safety issues and recognising the potential for serious harm.
- To ensure staff have received and read the E-Safety Policy, the Safeguarding and Child Protection Policy, the Code of Conduct and the Acceptable Use Policy and Agreement.
- To ensure that the E-Safety Policy, Code of Conduct and Acceptable Use Agreement are followed by Staff.
- Undertaking safeguarding training, off and online, in accordance with the statutory guidance.
- Taking overall responsibility for data management, and information security including GDRP compliance.
- Ensuring that effective information sharing arrangements are in place in cases where it is necessary for the protection of a child/children.

- Ensuring the school implements and makes effective use of appropriate ICT systems and services including filtering and monitoring.
- Ensuring Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety including filtering and monitoring.
- Ensuring necessary Risk Assessments are undertaken so that the curriculum meets the needs of the children, including risk of radicalisation.
- Ensuring that the school website meets statutory DfE requirements.
- When necessary, review and undertake a risk assessment for remote/home learning ensuring staff are reminded of the safeguarding implications of delivering home learning.
- Understanding the implications of a serious online safeguarding incident and ensuring Staff are aware of the procedure should this happen. Also that the necessary logs and records are kept.
- Staying up to date with the latest trends in online safety through regular updates.
- Ensuring staff have the necessary knowledge and training to carry out their online safety role.
- Ensuring that DfE guidance on sexual violence and harassment is followed across the school and that there is a zero tolerance approach to this, as well as to bullying.

6.3 Staff

Staff should be aware that use of the internet by themselves and pupils can be monitored and traced to an individual user and that they should set an example for the pupils in their use of the internet.

Staff must act with professionalism at all times and in accordance with the Staff Code of Conduct and the Acceptable Use Agreement.

Teaching and Support Staff are responsible for:-

- **Ensuring that they have read, understand and comply with the Safeguarding Policy, E-Safety Policy, Code of Conduct and the Acceptable Use Agreement (Appended to the Code of Conduct).**
- Inspiring and encouraging safe and responsible use of the internet at all times.
- Understanding that E-Safety is a core element of safeguarding and therefore it is everyone's responsibility**.**
- Completing a yellow Cause for Concern Form and passing it immediately to the DSL if they have any safeguarding concerns, including those relating to E-Safety.
- Ensuring the children are aware that they must tell a trusted adult, usually parent or Teacher, if anything they see online makes them feel worried, unsafe or scared.
- Following the escalation process if their concerns are not acted on promptly or satisfactorily.
- Identifying opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE curriculum, both outside the classroom and within the curriculum.
- When overseeing the use of technology, devices and the internet encourage safe, healthy use and monitor what children are doing and consider any potential risks they may encounter. Also consider the age appropriateness of the website being used.

- Closely supervising and guiding children in learning activities using online technology, supporting them with search skills, critical thinking and using age appropriate materials.
- Checking all online resources before using them in the classroom.
- When supporting children remotely, being mindful of additional safeguarding considerations.
- Encourage children to follow their Acceptable Use Agreement at home as well as at school.
- Taking a zero tolerance approach to bullying and low level sexual harassment.
- Being aware that they(staff) might over-hear online-safety issues expressed outside of the classroom - in corridors, the playground, toilets and other communal areas.
- Model safe, responsible and professional behaviour in the use of their own technology. This applies to outside of school, including social media, upholding the reputation of the school and the professional reputation of all staff.

6.4 Pupils

Pupils have a responsibility to:-

Read, understand, sign and follow the Pupil Acceptable Use Agreement (KS1 Appendix A, KS2 Appendix B). This applies does not apply to Reception.

- If home-learning is necessary, I will treat it as if I am learning in school and will behave as if a Teacher or parents is watching the screen.
- Understand the importance of adopting safe and responsible behaviours online when using digital technology out of school and that the Pupil Acceptable Use Agreement covers online activities out of school, including social media.
- Understand the importance of reporting abuse, misuse or access to inappropriate material while online.
- Know what action they should take if they or someone they know feels worried or vulnerable when using online technology.
- Understand the benefits and dangers of the online world and know who to talk to at school or outside of school if there is a problem.

Pupils in Reception have no independent access to the internet. All access is undertaken by the Class Teacher or Class Teaching Assistant and it is displayed on the class interactive whiteboard.

6.5 Parents

The school recognises that Parents/Carers have an essential role in ensuring that their children understand the need to use the internet in an appropriate way. The school will assist parents by providing information in newsletters and on the website.

Parents have a responsibility to:-

- Countersign the Pupil Acceptable Use Agreement and adopt the principles od this when their child is using technology at home.
- Consult the school if they have any concerns about their child's and others' use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their use of technology, including on social media.

- Ensure that, if their child is learning from home, they do so responsibly and that they adopt the principles of the Pupil Acceptable Use Agreement at home.
- Be aware that that it is prohibited to share any images (photos or video recordings) of children, other than their own, taken at school events and performances with the permission of the child's parents.

6.6 Visitors

Visitors are not permitted to use mobile phones in school so cannot use their phone to access the internet.

Any visitors who use their own laptops or other devices are expected to adhere to the principles of responsible and professional internet use. Any use of school technology is fully supervised by the member of staff hosting the visitor.

Any visitors that teach the children are required to complete a safeguarding form in advance which details the content of what they will be teaching. They are also closely supervised by the Class Teacher.

7.0 Access to Email by Pupils

7.1 There is provision in place to allow pupils access to email.

7.2 The sending of emails by pupils will only be done from and to approved email accounts and under the close supervision of the class teacher.

7.3 Emails sent to external organisations must be written carefully and approved by the Class Teacher before sending.

8.0 Video – Conferencing

8.1 Currently, pupils at The Bramptons rarely participate in video-conferencing.

8.2 When video-conferencing takes place it will be strictly under the supervision of the Class Teacher.

8.3 Particular vigilance concerning e-safety and safeguarding needs to be applied if the necessity to deliver remote learning requires the use of video based teaching.

9.0 Protecting Personal Data

9.1 Personal data will be recorded, processed, transferred and made available in accordance with the General Data Protection Regulations 2018.

9.2 Staff will ensure that any personal data regarding pupils that is held on portable devices such as laptops, is done so in a secure manner and in accordance with the Acceptable Use Policy and the Staff and Volunteer Code of Conduct.

10 Publishing Images of Pupils

10.1 Parents complete a consent form agreeing where photographs of their children can be published.

10.2 In accordance with the Staff Code of Conduct and Acceptable Use Agreement. photographs will only be taken on school cameras or ipads. Staff are not permitted to take any photographs of children on their personal devices, including mobile phones.

10.3 The children's names are never published with images unless express permission is given by a parent.

10.4 We do not have permission for any external organisations to take photographs of the children.

11.0 Emerging Technology

11.1 Emerging technologies will be examined for educational benefits and the use of them explored if felt appropriate.

12.0 Handling E-Safety Complaints

12.1 Complaints relating to misuse of the internet, including that relating to misuse by staff, are dealt with by the Head Teacher (Designated Safeguarding Lead).

12.2 Complaints of a child protection nature will be dealt with in accordance with Child Protection and Safeguarding procedures.

12.3 Cyberbullying will be dealt with in accordance with the Anti-bullying Policy.

13.0 Training

13.1 Staff will receive appropriate E-Safety Training and advice and support will be given to parents through awareness session and newsletters.

14.0 Related Policies

Acceptable Use Policy

Safeguarding Policy

Staff and Volunteer Code of Conduct

Remote Learning Policy

15.0 Equality Considerations

Some pupils with additional needs are provided with IT equipment in class, such as ipads, to support their learning across the curriculum.

There are no other equality considerations in relation to this policy.

KS1 Pupil Acceptable Use Agreement **Appendix A**

Name of Pupil:
Class:
To keep safe online:- ❖ **I only use the devices, apps, sites and games I am allowed to.** ❖ **I check with a trusted adult (Parent or Teacher) before using a new site, game or app.** ❖ **I ask for help if I am stuck or I am unsure.** ❖ **I tell a trusted adult if I am upset, scared or confused.** ❖ **I look out for my friends and tell someone if they need help.** ❖ **I know people online are not always who they say they are.** ❖ **I think before I click.** ❖ **I do not keep secrets or do dares and challenges because someone tells me to.** ❖ **I will use the same ways to keep safe online at home, as I do at school.** ❖ **I keep my body to myself when online.** ❖ **I do not share private information.** ❖ **I am kind and polite to others when online.**

My trusted adults are: **_____Home** **_____School _____Signed by Pupil**
I will encourage my child to adopt a safe and responsible approach to their online activity at home as well as at school, and I will model good online practices. **_____Signed by Parent**

KS2 PUPIL ACCEPTABLE USE AGREEMENT Appendix B

Name of Pupil:

Class:

To keep safe online by :-

- **Using the school internet and computers for school work and other activities to learn and have fun.**
- **Only using the devices, apps, sites and games I am given permission to use from a trusted adult.**
- **Not sharing anything that I know another person would not want sharing, or which might upset them.**
- **Keeping my passwords safe and asking for them to be reset if anyone finds them out.**
- **Thinking before I click on links or share to protect my online reputation.**
- **Understanding that some people may not be who they say they are.**
- **Not sharing private information.**
- **Keeping my body to myself when online.**
- **Not sending any photos without checking with a trusted adult.**
- **Asking to talk to a trusted adult if I feel upset, worried, scared or unsafe.**
- **By accepting and complying with the age restrictions and rules of some apps, games, websites and social networks.**
- **Being considerate, respectful and kind online.**
- **Never meeting anyone online that I do not know in real life.**
- **Saying "NO" if a friend asks me to do something online that I am not happy with.**

My trusted adults are:

_____ _____ **Home**

_____ **School** **Signed by Pupil**_____

I will encourage my child to adopt a safe and responsible approach to their online activity at home as well as at school, and I will model good online practices.

Signed by Parent_____