Foxhill Primary School

Policy on E-Safety and Anti-Cyber Bullying 2023-2024

1 Introduction

- The welfare and safety of children who attend our school is our paramount concern. We will promote the health, well-being and safety of the pupils in all we do. Our children have the right to protection, regardless of age, gender, race, culture or disability. They have a right to be safe in our school. The school understands the responsibilities set out under section 175 of the 2002 Education Act to work together in partnership with other agencies to help children to grow up in a healthy and safe environment.

- This policy draws on guidance for schools set out in: The Children's Act of 2004 Working Together to Safeguard Children DCSF 2006; Safeguarding Children and Safer Recruitment in Education DCSF 2007 Lord Laming *report on safeguarding 2009; Inspecting E-Safety The Briefing for Inspectors 2012; Keeping Children Safe in Education 2022*

2 Definition of safeguarding

- All adults who work with children have a duty to promote their welfare and keep them safe. The Children Act sets out these responsibilities as the requirement to keep children free from maltreatment, to prevent the impairment of children's health and development and to ensure that children grow up in circumstances consistent with the provision of safe and effective care.
- The breadth of issues classified within (e)Safety is considerable, but can be categorised into three areas of risk:

content: being exposed to illegal, inappropriate or harmful material
contact: being subjected to harmful online interaction with other users
conduct: personal online behaviour that increases the likelihood of, or causes, harm.'

3 Aims and objectives

- The aims and objectives of this policy are to ensure that all our staff promote safety when using the Internet, Email and mobile technologies, as well as promoting an anti-bullying message when using these means of communication. All pupils will know they are valued and their concerns will be taken seriously and addressed by the adults who care for them, via either children reporting problems, parents reporting problems or school council reporting problems. We want all children to feel safe and know what to do if they ever have concerns about any aspect of their physical or emotional safety.

- This policy sets out the roles and responsibilities of all adults who work or support our school and in so doing provides guidance on how we will make sure our school is a safe and caring place for all our pupils.

- We will ensure that this school works effectively with a wide range of agencies involved in the promotion of E-safety such as the community Police, schools partnership, Bradford Curriculum Computing Support and CEOP.

- This policy will outline the procedures we expect to happen if an incident of concern is identified with any child in our school. It will also set out how adults record and communicate concerns and how we will monitor incidents if and when they occur.

4 Staff responsibilities

It is the responsibility of the headteacher and E-Safety coordinator to ensure all of the following:

- that the governing body adopts appropriate policies and procedures to safeguard children in the school;
- that these policies are implemented by all staff;
- that sufficient resources and time are allocated for staff to carry out their responsibilities effectively;
- that all staff and adult helpers in the school are able to voice their concern if they feel that a child is vulnerable, or that there are any particular practices that are unsafe.
- To provide training for staff in E-Safety (TBC as Bradford Cyber Team no longer provides)

- All staff have a responsibility to report to the headteacher and the Computing Leader any concern they have about the safety of any child in their care as regards cyber bullying and E-safety. These incidents will be logged on paper and on CPOMS for the attention of the class teacher, E-Safety Leader and SLT, including Safeguarding Leads.

5 Safeguarding Procedures

- Any action taken by the Designated Safeguarding Lead when dealing with an issue of child protection must be in accordance with the procedures outlined in the LAs Child Protection guidelines.

- All adults in our school share responsibility for keeping our children safe. We may on occasion report concerns which, on investigation, prove unfounded. *(See Appendix C Inappropriate Material)*

- We will maintain accurate written records of all matters of concern from the date of this policy (See *Appendix A Record Log*) via CPOMS, where the Computing leader and class teacher also need to be tagged in, alongside Safeguarding leads.

- If teachers suspect that a child in their class may be a victim of E-safety or cyber bullying issues, or a child alleges an issue, they should not try to investigate, but should immediately inform the Computing leader, or Headteacher AND add to CPOMS. Abuse can be of a physical, sexual or emotional nature. *(See Appendix B for Guided to Dealing with Referred Incidents)*

- We have a system of logging onto the network using personal log-ins and passwords, rather than shared passwords. This is for all staff and children in KS2. The younger children in Year 2 have individual usernames. Year 1 and Foundation Stage children continue to have class log-ins. Children have been taught how to create a 'strong' password.

- Confidential data such as planning, SEND documents and Assessments are stored in a shared drive which children cannot access.

- Teachers have an encrypted (password protected) USB stick, an encrypted home laptop and are encouraged to use One Drive via their school email address, which is the address to be used for work matters.

- We are made aware when a child enters school if they cannot have their photo or video taken via the GDPR declaration form (see GDPR policies).

- Children are issued with an Acceptable Use Policy at the start of Reception, KS1 and KS2 which they take home. They sign-up by returning a signed slip and non-returns are chased via text messages. The AUP covers the acceptable use of ICT equipment, behaviours when online and use of the Internet. *(See Appendix D AUP).* A simplified version is available for KS1. (*See Appendix E AUP)*

- We have a Staff Acceptable Use (of the Internet and equipment) policy (AUP) to be implemented each September. In addition there will be a brief visitor and governors AUP to be displayed on the sign-in screen (*See Appendix F)*

    - The E-Safety coordinator has registered the school to work towards the 360^0 E-Safety Mark which recognises 3 levels of good practice through an accreditation. We are working towards completing level two.

    - Radicalisation – Action has been taken, via staff training, to reduce the risk of radicalisation and extremism, including how this may link to use of the Internet.

6 Teaching and learning

- An E-safety survey is completed by each class to highlight the activities, views and understanding of the children. This will be done prior to E-Safety Week so the results can feed into the planning and another completed at the end to evaluate learning.

- E-Safety homework will be provided to encourage parental engagement in their child's awareness.

- Our teaching of PSHE (SCARF) helps to develop appropriate attitudes in our children, and makes them aware of the impact of their decisions on others. We also teach

them how to recognise different risks in different situations, and how to behave in response to them.

- We will teach in such as way as to encourage pupils to be able to voice their opinions and develop their own self confidence. We aim to build strong and caring relationships with all our pupils. In so doing we hope to provide our pupils with the skills necessary to be able to bring to the attention of any adult working in the school any matters of concern they may have. We will always take seriously any safeguarding issues drawn to our attention by any pupil.

- Reception to Year 6 have a programme of study for Internet Safety learning, both stand alone within Safer Internet Week, and within Purple Mash, where knowledge progresses throughout the Curriculum. This is based on progression within the South West grid for Learning, alongside other E-Safety agency resources, as recommended by Bradford Computing Consultants. In addition, children are taught the SMART rules (Safe, Meeting, Acceptable, Reliable,Tell) and about the CEOP report button. This scheme is updated as new guidance is received

- A permanent display in the ICT Suite highlights the E-Safety messages and displays celebrates children's work. Each class has E-safety posters displayed.

- A dedicated Parents E-Safety page on the website includes facts sheets about social media, apps and games. Regular updates are sent home depending on information we receive about current E-Safety issues.

- The updated school website includes links for Parents and children to teach the important E-safety in the Keeping Safe and Children's sections of www.foxhillprimaryschool.co.uk.

- An annual competition for the children makes the week more high-profile.

7 Resources

Resources to be used on the 'E Safety Week include:

- A range of picture books and short stories, appropriate for each class – for use on Safer Internet Day and throughout the Year for Y5 and 6 children.
- Range of video clips, activities and lesson plans (from CEOP and other E-Safety organisations)
- Bradford Innovations Centre and South West grid for Learning progressive scheme of work
- Posters in classrooms
- Assembly
- Display in a central corridor
- Desktop image competition

- Monitoring software has been purchased (Smoothwall Monitor) which monitors typing entries. This will highlight any E-Safety issues in Internet searching and typing by anyone in school and a weekly report is sent to the E-Safety Leader, Safeguarding Lead and Headteacher.

8 Confidentiality

- We regard all information relating to individual cases of cyber-bullying or E-safety as confidential between SLT, Teacher, E-Safely Leader, parents and child involved.

9 Continuing professional development and staff training

- The Computing Leader and has regular training and development opportunities so their skill and competence level remains high. She has been trained according to the CEOP award by Bradford Consultants.

- We aim to provide annual CPD to staff to raise their awareness of E-safety issues, and to improve their knowledge. This will be sourced by in 2023 as Bradford PCSO Team no longer provide.

10 Allegations

- If an allegation of cyber bullying is made, it will be investigated by the Headteacher. In the case of an E-Safety issue, arising in school, or from a parental concern , again the Headteacher will investigate the situation and act in accordance with the safe-guarding policy. This will be logged on CPOMS so we can respond with appropriate training for children from either staff or the Bradford E-Safety PCSOs.

11 The Leadership and management of safeguarding

- All members of staff have a part to play in ensuring that our pupils are safe and that their wellbeing is supported.

- The Computing Coordinator will have responsibility for maintaining an up-to-date knowledge of E-safety issues and teaching programmes required and liaising with external agencies. She will also oversee the training programme for all staff and ensure that staff are kept up to date with all relevant parts of our safeguarding policy.

Monitoring and review

- The Computing Leader and Headteacher take lead responsibility for dealing with E-safety.
- This policy will be reviewed annually by the Computing Leader.

Reviewed	July2023
Approved at the Governors meeting on	13th July 2023
Signed	*R Hainsworth*
Date of next review	July 2024