LITTLE HEATON CE PRIMARY SCHOOL

E-SAFETY POLICY

Mark 9.23 - ***All things are possible for those who believe.***

Learning Together We Grow in Faith

Date of Issue: ***April 2023***	Date of Last Review: ***January 2022***
To be Reviewed: ***April 2025***	
Headteacher Signature:	Chair of Governors Signature:

LOVE RESPECT RESILIENCE ASPIRATIONS TRUST HONESTY

OVERVIEW

This school has invested over the last few years in information technology and computer systems to support teaching and learning and to give learners the opportunity to seek information and carry out research. Access to the internet carries with it the danger that learners could find and view material that is unsuitable for them or that they could be put at risk from cyber-bullying, unwanted and inappropriate contacts. This policy seeks to ensure that the school network, internet and other forms of information communications technology is used appropriately for learning but with safeguards to protect learners from harm. This policy complies with statutory safeguarding guidance and our own Safeguarding Policy and agreed procedures.

INTENT

- To ensure that learners' access to inappropriate sites and locations is restricted.
- To ensure that the use of the Internet is for proper purposes related to the teaching, learning and curriculum of the school.
- To protect children from harm and upset that could be caused through giving them access to inappropriate sites, materials, images and contacts.
- To make learners aware that there are inappropriate sites that are harmful and so must be avoided in school and at home.
- To encourage learners to report immediately any inappropriate, sites, materials or contacts that they find on the Internet either at school or at home.
- To ensure that pupils do not suffer from abuse by other pupils, including abuse by sexting.
- To ensure that the school complies with section 127 of the *Communications Act 2003* and the recommendations of the *Byron Report 2008*.

IMPLEMENTATION

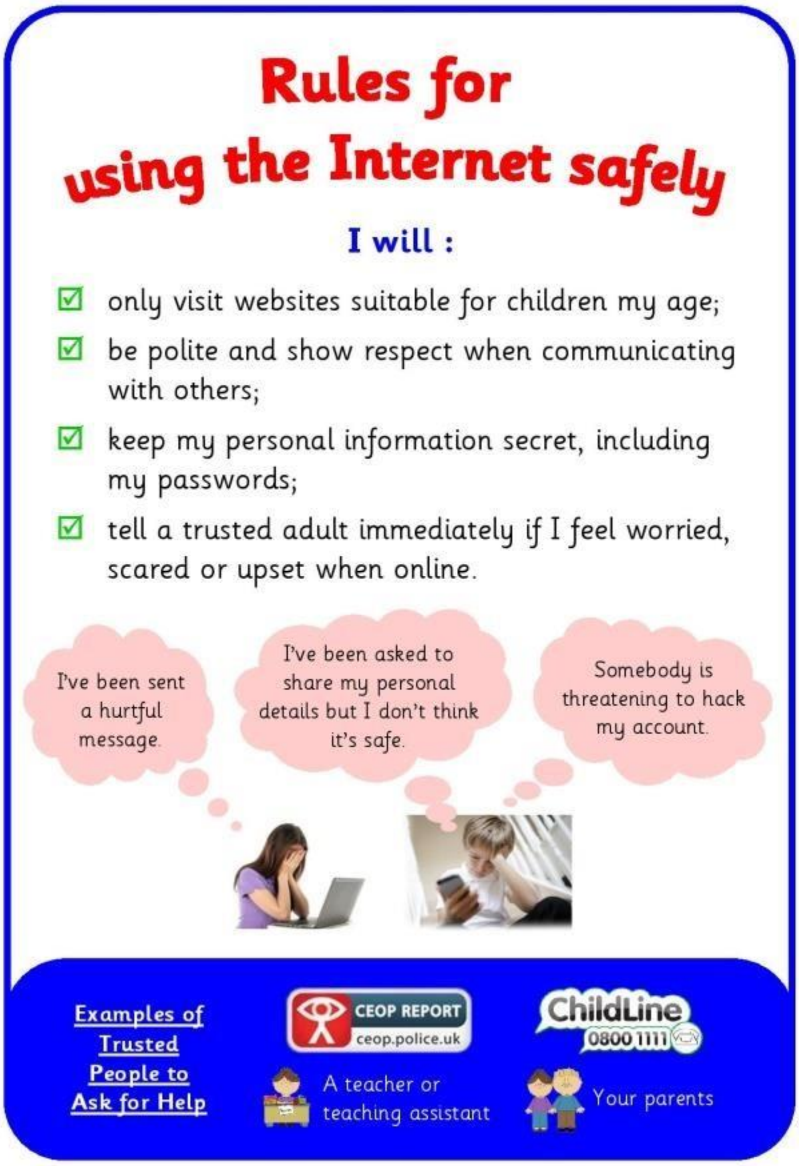
- Appropriate Firewalls are put in place and must be enabled at all times on all the school computers.
- Staff must not disable or bypass Firewalls on any school owned computer under any circumstances or at any time.
- Learners must be supervised by adults at any time that they are given access to the Internet.
- Staff must only use computers for school purposes. School computers used by staff either at home or in school must not be modified or used for personal use.
- Learners must be encouraged to notify staff if they at any time come across unsuitable material on a computer or if they feel threatened or harassed by any form of cyber-bullying.
- Staff must notify the headteacher immediately if they find unsuitable or inappropriate material on a computer, mobile phone or storage device or if they find that a learner is the subject of cyber-bullying.
- Spot checks and audits will be carried out from time to time to ensure that computers are being used appropriately.
- Incidents of inappropriate use of ICT or of cyber-bullying will be reported to the headteacher and records will be kept.

IMPACT

Learners and staff will be able to enjoy and use of ICT to enhance teaching, learning and the curriculum and to access useful educational information and materials, without risk of harm or upset.

APPENDIX – PUPIL RULES FOR INTERNET USE

Educational use of the internet is characterised by activities that provide children with appropriate learning experiences. In accordance with the *RSN Acceptable Use Policy*, clear rules which help children develop a responsible attitude to the use of the Internet have been devised. These expectations regarding the use of the Internet will be explained to all classes (e.g. in Computing and PSHE lessons) and are displayed prominently around the building.



Rules for using the Internet safely

I will :

☑ only visit websites suitable for children my age;

☑ be polite and show respect when communicating with others;

☑ keep my personal information secret, including my passwords;

☑ tell a trusted adult immediately if I feel worried, scared or upset when online.

I've been sent a hurtful message.

I've been asked to share my personal details but I don't think it's safe.

Somebody is threatening to hack my account.

Examples of Trusted People to Ask for Help

CEOP REPORT ceop.police.uk

ChildLine 0800 1111

A teacher or teaching assistant

Your parents

Children are provided with personal accounts for several online services, such as Purple Mash, Times Tables Rockstars, Epic Reading, Microsoft Office 365. They are regularly reminded of the need to ensure that no unauthorised people gain access to any of their accounts – by choosing strong passwords and always logging out when finished, for example.