Ashleigh

Primary School.

E-Safety

 Policy

Reviewed October 2021

Agreed by staff: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved by Governors: \_\_\_\_\_\_\_\_\_\_\_\_

Review date: October 2023

**British Values**

Through its curriculum, extra-curricular activities, teaching and learning this school will promote British values. By doing so, we will ensure that all learners understand the values that have traditionally underpinned British society. The teaching of these values will promote cohesiveness within our school and community. We will prepare pupils for life in England where the population has an increasingly rich diversity of backgrounds, origins, beliefs and cultures by promoting the values on which our society has been built. By teaching pupils these values we will help all to become good citizens of the United Kingdom of Great Britain and Northern Ireland.

**Race Equality and Racial Harassment**

Implicit in all our policies is a belief in race equality and everything will be done to promote this. We do not tolerate racial harassment. (Refer to School’s Race Equality and Racial Harassment Policies).

**Using new learning technologies effectively and safely**

**Contents**

**Safety Audit**

**Teaching and Learning**

**Managing Internet Access**

**Staying Safe**

**Policy Decisions**

**Communications Policy**

**Use of Technology in Primary School**

**Useful Sites and Resources**

Our e-safety Policy has been written by the school, building on the Blackburn with Darwen policy that has been adapted from Kent’s Children Families and Education Directorate draft policy, following Becta guidance. It has been agreed by the senior leadership team and approved by Governors. It will be reviewed annually.

 **Writing and reviewing the e-safety policy**

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

* Ian Matthews is the schools e safety co-ordinator who will work in collaboration with the child protection co-ordinator.
* Our e-Safety Policy has been written by the school, building on the Blackburn with Darwen amended version of the Kent e‑Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
* The e-Safety Policy and its implementation will be reviewed annually or in response to an incident.
* The e-Safety Policy was revised by Leadership Team
* It was approved by the Governors on: March 2015

Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

|  |  |
| --- | --- |
| Has the school an e-Safety Policy that complies with Becta guidance? | **Yes** |
| Date of latest update: **October 2021** |
| The Policy was agreed by governors on: **October 2021** |
| The Policy is available for staff at: **T drive on the school server** |
| And for parents at: **www.ashleighdarwen.co.uk** |
| The Designated Child Protection Coordinator is: **Ian Matthews** |
| The e-Safety Coordinator is: **Ian Matthews** |
| Has e-safety training been provided for both students and staff? | Staff – Sept 2021Pupils – Autumn 2021 |
| Do all staff sign an ICT Code of Conduct on appointment?  | Yes |
| Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?  | Yes  |
| Have school e-Safety Rules been set for students?  | Yes  |
| Are these Rules displayed in all rooms with computers? | Yes  |
| Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access  | Yes |
| Has an ICT security audit been initiated by SMT, possibly using external expertise?  | Yes |
| Is personal data collected, stored and used according to the principles of the Data Protection Act?  | Yes  |
|  |  |
|  |  |

**Teaching and learning**

**As the children’s access and understanding expands, so should the guidance and rules to ensure safe access use of the internet**

**Why Internet use is important**

* The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality 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 evaluate Internet content appropriate to their age.**

* The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
* Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
* Sanctions for inappropriate use of the internet will be explained to the children.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Managing Internet Access**

**Information system security**

* School ICT systems capacity and security will be reviewed regularly.
* Virus protection is updated regularly.
* Security strategies will be discussed with Blackburn with Darwen.

**Managing filtering**

* The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, it must be reported to the e‑Safety Coordinator and the LA will be informed so that they can take appropriate action.

**Staying safe**

The school will ensure that pupils and parents are aware of e safety issues. A list of useful addresses and resources is included in this document.

* The school internet access is designed expressly for pupil use and includes appropriate filtering.
* Pupils may only use approved digital methods of communication on the school system e.g. not forwarding chain letters.
* Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
* Pupils and staff will use equipment responsibly.
* Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
* Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.

**Published content**

Any information that can be accessed outside the school’s intranet should be classed as published whether in electronic or paper format.

* Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
* General contact details should be the school address, e-mail and telephone number. Staff or pupils’ personal information will not be published.
* The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing pupil’s images and work**

* Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.
* Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
* Pupils’ full names will not be used anywhere, particularly in association with photographs.
* Written permission from parents or carers will be obtained before photographs or video of pupils are published.
* Where pupil’s work is published the school will ensure that the child’s identity is protected.

**Managing emerging technologies**

* The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

**Protecting personal data**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**Policy Decisions**

**Authorising Internet access**

* All staff must read and sign the ‘Responsible ICT Use Agreement’ before using any school ICT resource.
* The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.
* Parents will be asked to sign and return a consent form.

**Assessing risks**

* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
* The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

**Handling e-safety complaints**

* Complaints of Internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA.
* Any complaint about staff misuse must be referred to the headteacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Pupils and parents will be informed of the complaints procedure on request.

**Communications Policy**

**Introducing the e-safety policy to pupils**

* E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
* Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

**Staff and the e-Safety policy**

* All staff will be given the School e-Safety Policy and its importance explained.
* Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
* The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

**Enlisting parents’ support**

* Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the learning platform.

Chair of Governors: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Headteacher: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_