Embleton Vincent Edwards C of E Primary School

Policy	Online Safety	
Policy Number	P019	
Ratification Date	September 2019	
Review Date	Autumn 2021	
Signed		Chair of Governors

At the school we fully endorse the view that ‘every child matters’ and our school seeks to ensure that its provision fully supports this philosophy.

Whilst recognising and respecting the wide variety of beliefs held by our children and their parents, and their diverse backgrounds, at the core our ethos is to provide an environment where children are given a framework to make moral choices throughout their lives, not just during their school years.

Embleton Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Teaching and learning

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. Internet use will enhance learning. The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils; pupils will only use the student server to access the internet. Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils are taught how to evaluate internet content, including ‘fake news’. The use of internet derived materials by staff and by pupils complies with copyright law.

Information system security

School ICT systems capacity and security are reviewed regularly. Our School IT Technician is employed by NCC. Virus protection is installed on all school systems and is updated regularly. Advice on security strategies is sought from the Local Authority and implemented in school by the IT technician or staff as appropriate. The school buys in to an SLA which gives reports on internet usage, including keywords and sites visited. This is reviewed weekly by the e-safety coordinator.

E-Safety Training

Staff, and children train regularly on aspects of e-safety. Parents and governors to be invited to training annually. The school has a named e-safety governor - **Mr Mark Green** and e-safety coordinator - **Mrs Nicola Threlfall**.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail 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.
- The forwarding of chain letters is not permitted.
- Children are to be made aware of any new e-safety provision.
- E-safety is a topic which is taught regularly across the school year.

Published content and the school website

The contact details on the website are limited to the school address, e-mail and telephone number. The only personal information for staff and governors given out are their names. Pupils are only ever referred to by their first name.. The headteacher takes overall editorial responsibility and ensures that the content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified unless written parent permission has been sought. Pupils' full names will not be used anywhere on the website particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The LA filtering system blocks access to social media/blog/video sites. This is with the exception of facebook, twitter and youtube which are enabled on the staff server only.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space, unless as part of a lesson, and only when directed by an adult.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others.

Managing filtering

The school works in partnership with the LA, Department for Education 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.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff will only use the school phone when contact with pupils or their family is required (this is waived in an emergency when staff are off school property. Whilst contact via the school is preferable, if this is not feasible then contact can be made via a member of staff's mobile phone. When this happens, the event must be logged with the e-safety coordinator.)

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.

Policy Decisions Authorising Internet access

All staff, volunteers and pupils sign an Acceptable Use Policy before they are allowed access to the school ICT systems. The school maintains a current record of all staff and pupils who are granted access to school ICT systems. Parents sign and return a consent form allowing their child to access ICT in school.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of internet access.

The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

The headteacher receives a weekly print out of websites accessed, phrases logged and user details. This is scrutinised and any issues dealt with promptly.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by the headteacher. 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.

Community use of the internet

The school does not currently allow community use of the school internet system. Should this change the school will liaise with local organisations to establish a common approach to e-safety.

Professional use of the internet

A variety of professionals require to use the internet as part of their work within the school. They are given a specific visitor log-in to do so. All those given the log in are required to sign to say they agree with the Acceptable Use policy.

Communications Strategy

E-safety policy and procedures are introduced to pupils, parents and staff through training. Age appropriate e-safety rules are posted in all networked rooms. Pupils are informed that network and Internet use will be monitored.

Staff and the e-Safety policy

All staff sign as having read the e-Safety Policy annually. Its importance is explained during training. Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The headteacher manages filtering systems and monitors ICT use.

Enlisting parents' support

Parents' are kept informed of e-Safety through the website, newsletters and during workshops and parent meetings. Concerns about particular websites, apps or games that the children talk about are brought to the attention of parents as soon as is practicable.