Bader Primary

E-Safety Policy

2016

This policy has been designed at Bader Primary School with both staff and pupil input.
January 2016

Our Vision for Technology at Bader Primary School

At Bader Primary School, we would like to use technology as a tool to help the children progress further in their learning. We want to give them the skills they need in the future to become independent learners with the help of technology.

In addition to this, we also want to share learning more efficiently with parents. We aim to use technology to allow children to take home and share their learning as well as share any assessment information and goals with parents.

E-Safety in the Curriculum

As part of our curriculum, children will be educated in the importance of E-safety across all year groups and different subject areas, for example PSHE. As well as this, within the Bader School Computing Curriculum each strand has a relevant E-Safety and Copyright focus.

In addition to this, any year groups with 1:1 devices implemented will take part in a 5-day initial E-safety week. This will cover safety online, what to do if you have a concern, your digital footprint, downloading and use of images online. Children will also be introduced to the 'Thinkuknow' website in order to support them with any concerns.

Cyberbullying

Cyberbullying will be explicitly addressed with each class and all children will be introduced to the consequences and procedures around cyberbullying.

- **If cyberbullying is conducted using a school device;**
  - This will be recorded on the child's record using CPOMS.
  - Parents/Carers will be asked to come into school and discuss the incident
  - For two weeks the use of the device will remain supervised
  - The child's device will be checked each school day by a member of staff and each weekend day by a parent/carer

- **If cyberbullying is conducted using a non-school device;**
  - This will be recorded on the child's record using CPOMS.
  - Parents/Carers will be asked to come into school and discuss the incident

A definition of cyberbullying is:

'The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.'

Management of Internet Access

Within school the internet is provided by Stockton Local Authority and managed by ONEITSS. In addition to this GoGuardian is used to monitor and track the 1:1 devices both inside and outside of school. Both staff and parents, however, have been made aware that all use of devices should be supervised and monitored.

The internet provides an invaluable amount of opportunities within our curriculum due to its open nature. It allows for independent learning, collaboration and the sharing and publishing of children's work online. In addition to this we aim to use the internet to strengthen the bond between home and school, sharing children's progression and targets with parents/carers. It is the open nature of the internet however that can pose a risk to children.

In order to keep children safe online, the following are in place:

-All staff are aware that any recommended websites given to children should be thoroughly checked by the teacher first.
-Children's names should not be entered into any internet-based software without consulting the E-Safety team.
-All internet use is supervised, this includes children's access to devices during playtime or lunchtime.
-Children receiving devices will take part in initial training on e-safety.
-In the case of take-home devices parents will be advised to check on their children's browsing history regularly and supervise children on devices
- If staff/students find an unsuitable site accessible in school then the screen must be switched off or the device must be closed and it must be reported to the E-Safety team.
-Staff and students are aware that all school based email can be monitored
-Children are aware that all use of devices is monitored
-All staff, parents and students must have signed an acceptable use agreement prior to using internet based software

Photos and Images of children

When joining the school parents are asked to give consent for images of children to be published- a list of children who do not have this consent will be available on the school learning platform.

It is advised that all photos of children are taken on school devices, in the case of a school trip photos may be taken on alternative devices but must be uploaded to their intended place of use and then removed from the device before the end of that trip.

Children may not upload images of themselves or other children without permission of their class teacher.

Roles & Responsibilities for E-Safety

It is the responsibility of every member of staff within the school to report any e-safety issues they have witnessed. Any e-safety issues should be reported immediately to the e-safety team which consists of the Digital Technology Lead and the Headteacher. These will then be logged using cpoms.

It is the responsibility of each class teacher to ensure that E-Safety is covered in accordance with the computing curriculum which is available on the learning platform.

In the case of devices being taken home it is the responsibility of the parent to regularly check what the child is doing on their device. Parents are made aware of this responsibility on initial sign up to devices.

Email within School

The use of email within school is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or externally. We recognise that pupils need to understand how to style an email in relation to their age. The 2013 National Curriculum states use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Social networking and Digital Footprint

All access to social networking sites will be blocked within school for pupils. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils will be educated on safe use of social networking and the implications of their digital footprint in order to prepare them for use of social networking in the future.

Emerging Technology

Emerging technologies will be examined for educational benefit by a member of the E-safety team and the risk assessed before use in school is allowed.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual.
The Act grants individuals rights of access to their personal data, compensation and prevention of processing. http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Please could all staff read and sign the slip below then return to the Digital Technology lead.

I have read and agree to the Bader Primary School E-Safety Policy.

Signed:_____

Date: _____

Policy Review Date: September 2017