E-Safety Policy

February 2018

Revised: May 2018

Review: May 2020

Safeguarding and E-Safety

At Bader we believe that every child and adult is equally respected and accepted. Staff and Governors are concerned that all aspects of school life are "fair" and "safe" for children, staff, parents/carers and the wider community. ***We aim to give all children the skills they need, now and for the future, to embrace and adapt to an ever-changing digital world.***

E-Safety is that area of Safeguarding that deals with the acceptable behaviour needed to achieve a safe and harmonious online community. It teaches users of the Internet, social media and connected devices what to do should they encounter difficulties or distressing experiences.

The aims of this policy is to:

● Through consultation with pupils; establish the ground rules we have at Bader Primary School for using the Internet and electronic communications. It highlights the need to educate pupils about the benefits and risks of using digital technology and provides safeguarding protocol and awareness for all users to enable them to use the internet safely and respectfully.
● Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
● To understand that accessing inappropriate sites accidentally or being subject to distressing content is not something to feel guilty about and that any such incident should be reported to staff/parents immediately.

E-Safety

E-Safety is the duty of staff, parents and the children. We educate our children to practise that all users of the internet should be respectful, and that the same standards of safety, equality and acceptable behaviour that apply in our communities, is also applied online.

As a community we aim to recognise and guard against bullying, intimidation, discrimination, grooming and exploitation of vulnerable users. E-Safety is an important part of keeping children safe at Bader Primary School. We have extensive security measures and safe working practices in place

'Aiming HIgh'

in school, which are monitored both internally and externally, to help safeguard pupils from potential dangers or unsuitable material.

In school children are taught how to stay safe and behave appropriately online. Parents and Carers are reminded, guided and strongly encouraged to educate children on what to do if and when they encounter danger and how best to deal with it. As a school, E-Safety incidents are dealt with in accordance with our policies. Sanctions are used to deal with unacceptable behaviour and serious incidents are escalated to the appropriate authorities.

Working together:

We can only be successful in keeping children safe online if staff and parents work together to ensure the E-Safety message is consistent. It is important that adults speak to their children about how they can keep safe, teach them how to behave appropriately online, set rules and deal accordingly with inappropriate or dangerous behaviour.

Introducing the e-safety policy to pupils

- E-safety rules are posted around the school environment and in the Mac Suite. These rules are reviewed and discussed with the pupils at the start of each year.
- Pupils are informed that network and Internet use will be monitored.
- All pupils have access via the Learning Platform to the child exploitation and online protection centre: http://www.thinkuknow.co.uk/. This website is also used during e-Safety/PSHE lessons.

Management of Internet Access

Within school the internet is provided by Aspire via One IT and managed by Conyers I.T. department. In addition to this GoGuardian is used to monitor and track the chromebook devices both inside and outside of school. Both staff and parents, have been made aware that all use of devices should be supervised and monitored.

Parents cannot solely rely upon schools systems for all potential E-safety issues. All parents and carers are responsible for the use of the internet at home - ensuring it is safe, appropriate and monitored - via parental controls, conversations with their child and regular checks on the content accessed by their child.

The internet provides an invaluable amount of opportunities within our curriculum. It allows for independent learning, collaboration and the sharing and publishing of children's work online.

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

‘Aiming HIgh’

- 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 Senior Leadership Team.
- All internet use on the school premises is supervised, this includes children's access to devices during playtime or lunchtime.
- All children will take part in E-safety assemblies and class focused lessons.
- In the case of chromebooks, parents are advised to check on their children's browsing history regularly and to supervise children on their device.
- If staff/students where to find an unsuitable site accessed in school, then the screen must be switched off immediately, the device must be closed and the matter must be reported to the headteacher and E-Safety coordinator.
- Staff and students are aware that all school based email can be monitored.
- Children are aware that all internet usage is monitored and regulated.
- All staff, parents and students must have signed an acceptable use agreement prior to using internet based software.
- Children are taught, through assemblies and within the Computing Curriculum, to recognise that they are responsible for their own 'digital footprint'. All searches and content viewed online is traceable; school systems cannot block everything - children and parents cannot rely only upon the filtering and school security systems to keep children safe online.

School website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher is responsible for the content and editorial choices; facilitated by Conyers I.T. department.
- Pupils' full names are not used anywhere on the Website.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school Website.

Photos and Images of children

When joining school, parents are asked to give consent for images of their child/children to be published digitally or around the school environment. A list of children who do **not** have this consent is available on the school learning platform via google drive.

All photos of children must be taken on a school device managed by the school. **Staff should not use their own personal devices to take photos of children.** In the case of a school trip the school will provide a school iPad to take and store any photographs.

Children may not upload images of themselves or other children.

<p align="center">***'Aiming HIgh'***</p>

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 or had knowledge of - (*please see Staff Acceptable use policy*). Any E-safety issues should be reported immediately to the Headteacher. All matters of E-Safety should be recorded using CPOMS.

It is the responsibility of each class teacher to ensure that E-Safety is covered in accordance with the statutory requirements of the computing curriculum.

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

- **Staff are required to ensure that all social media profiles are sufficiently secure and set to private to protect their own privacy and professional integrity. With this in mind, staff are not permitted to accept any request by a child to 'friend' a member of staff and in the event that this should happen, staff must report this immediately to the Headteacher and using CPOMS. Any form of online connection with children who attend the school is strictly prohibited and may lead to disciplinary action. Furthermore, school does not encourage online connections with parents; although, there may be exceptions whereby staff have friends or family who are parents. In this case, staff must uphold their professional responsibility to ensure that school information and data are not compromised.**

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 National Curriculum states that children should learn to 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.

Staff must only use their school email in order to communicate on a professional basis and never to respond to any email that may have originated from a pupil's private address or any unfamiliar source.

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 the Conyers I.T. department and the E-Safety coordinator, then risk assessed before use in school is permitted.

Please could all staff read and sign the slip below then return to the Headteacher.

All members of staff are required to familiarise themselves with this policy as part of their induction programme.

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

Signed:_____

Date: _____

Policy approved

Date _____

Signed _____ (Chair of Governors)

The EU General Data Protection Regulation (GDPR)
https://www.eugdpr.org/eugdpr.org.html

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR).

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time those organisations in non-compliance may face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

The GDPR requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual.