



E-Safety Policy

Revised: February 2021

Review: February 2023

This policy was written by the E-Safety Coordinator, Mrs H. Mudgway (Computing Subject Leader) in consultation with Mr C.Coleman (Director of I.T. systems and Assistant Headteacher of Conyers School)

The Designated Safeguarding Lead is Mrs S. Jatwa (Deputy Headteacher).

Our E-Safety Policy has been written by the school and seeks to incorporate the current government guidance. It has been agreed by the senior leadership team and ratified by the school governing body. The E-Safety Policy for Bader Primary School will be reviewed every two years. This policy will next be reviewed February 2023.

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 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 in classrooms and in the IT Suite. These rules are reviewed and discussed with the pupils at the start of each year.
- Pupils are informed that all network, device and Internet use is monitored.

Management of Internet Access

Within school, the internet is managed by The 1590 Trust IT Services. Staff, pupils and parents are aware that all use of devices is supervised and monitored.

The internet is filtered and managed by The 1590 Trust IT Services, and so inappropriate material and content, including pornography, will not be accessible by pupils.

In the case that any inappropriate content is accessed, pupils will need to alert a member of staff immediately. This will be reported to The 1590 Trust IT Services and to SLT, and logged on CPOMS.

In the event that inappropriate material is accessed deliberately by a pupil, this will be reported to The 1590 Trust IT Services and SLT, it will be logged on CPOMS, and parents / carers will be notified.

If staff have any concerns regarding E safety / safeguarding issues, this will be reported to SLT immediately and logged on CPOMS.

Parents cannot solely rely upon school 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.

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 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.
- If staff or pupils were to find an unsuitable site accessed in school, the matter must be reported to a staff member immediately, and the headteacher and E-Safety coordinator will be informed.

- Staff and pupils are aware that all internet usage, including school based email or messages, is monitored and regulated.
- All staff, parents and pupils must have signed an acceptable use agreement prior to using internet based software.
- Pupils are taught, through assemblies, Anti-Bullying Week, Internet Safety Day, and within the Computing and PSHE Curriculum, to recognise that they are responsible for their own 'digital footprint'.
- School systems cannot block everything - children and parents cannot rely only upon the filtering and school security systems to keep children safe online.

Monitoring and appropriate use of remote systems

Seesaw:

- Seesaw is used for children in school and at home to post learning activities to their teacher.
- Photographs of other children will not be posted on an individual's Seesaw journal.
- Seesaw is used to post learning activities only; children should not send photographs which are not linked to their learning.
- All posts must be approved by the teacher before it appears in a child's journal.
- Comments on their own or another child's work are permitted, but must be approved by the teacher.

Zoom:

The following expectations are agreed upon by parents/carers and pupils, prior to joining a Zoom call:

- You are at 'virtual school,' and the same school expectations are in place throughout our Zoom Assembly.
- You must be fully dressed and ready, when logging in to the assembly.
- Make sure your device is in an open environment, not in a bedroom, and do not move it during the assembly.
- You must join with your full name. Any abuse or misuse will lead to disconnection; you will not be able to re-enter the assembly. Your camera must be switched on and your face must be visible. You will be disconnected from the Zoom if you are not visible.
- Your microphone will be muted. You should only unmute if you are asked to, or if your teacher has unmuted you.
- Assemblies will be recorded. The recording will be stored safely on Google Drive.

Twitter:

- School will only post images of children who have had photo permission from parents / carers.
- A child's name will not be posted on Twitter, particularly when used alongside a photograph of them.
- Twitter is used to celebrate the learning and ethos of the school, and to showcase our Bader Values and enriched curriculum.

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 The 1590 Trust IT Services.
- 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.

Photographs that include pupils will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the school website or Twitter, particularly in association with photographs.

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

Pupils may not take or upload images of themselves or other children, unless asked to do so by a member of school staff.

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. Any E-safety issues should be reported immediately to the Headteacher and E-Safety coordinator. 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 iPad devices being taken home, it is the responsibility of the parent to regularly check what the child is accessing on their device. Parents are made aware of agreements when signing out a device from school. Use of iPads at home will also be monitored by school.

Staff use of Social Media

Staff are required to ensure that all social media profiles are **sufficiently robust** and set to private to protect their own privacy and professional integrity.

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, E-Safety coordinator and using CPOMS.

Any form of online connection with children who attend the school is strictly prohibited and may lead to disciplinary action.

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

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

- The school blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Our pupils are asked to report any incidents of cyberbullying to the school.
- School staff are advised not to add children, or parents as 'friends' if they use these sites.
- 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.

Managing Emerging Technology

Emerging technologies will be examined for educational benefit by The 1590 Trust IT Services and the E-Safety coordinator, then risk assessed before use in school is permitted.

Pupils are not allowed to bring personal mobile devices/phones to school.

The sending of abusive or inappropriate social media messages, text messages or emails outside school is forbidden.

Acceptable Use Policy

This E-Safety policy works alongside our Acceptable Use Policies, which have been signed by parents/carers, pupils and staff.

Staff and the e-Safety policy:

All staff must sign the Staff AUP and a copy is kept on file.

Any information downloaded must be respectful of copyright, property rights and privacy.

All members of staff are aware that internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

An iPad issued to a member of staff remains the property of the school.

Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Parents and the e-safety policy:

All parents will be asked to sign the AUA (Acceptable Use Agreement) for pupils, giving consent for their child to use the Internet in school by following the school's e-Safety eSafety policy.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or Twitter.

Protecting personal data

The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school.

The school will hold personal information on its systems for as long as individual members of staff remain at the school, and remove it in the event of staff leaving or until it is no longer required for the legitimate function of the school.

Each staff member has the right to view personal information that the school holds and to have any inaccuracies corrected.

We will ensure that all personal information supplied is held securely, in accordance with the General Data Protection Regulation (GDPR).