Broadwood Primary School

E-SAFETY POLICY

Last reviewed	May 2024
Reviewed by	Curriculum Committee
Next review date	September 2024

This policy applies to all members of the school community - including staff, children, parents/carers, visitors, volunteers - who have access to Broadwood Primary School's ICT system, both in and out of the school.

What is E-Safety?

E-safety means *Electronic Safety*. As the use of technology is becoming more substantial in the lives of children, it is crucial they are aware of both the benefits and potential dangers. Technology can be a fantastic tool to enhance teaching and learning, and at home it can also influence and change the way children live and the activities they choose to partake in. Technology is the future and using it safely is of the highest importance.

This policy sets out responsibilities and procedures taken by Broadwood primary school to ensure the safe use of technologies by our entire school community.

Our E-Safety Policy has been written by school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's E-Safety Lead is Mrs Laurie Underwood
- The E-Safety Governor is Mr David Jones
- The E-Safety Policy and its implementation will be reviewed on an annual basis.

Roles and Responsibilities

Governors:

All Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Lead (at least annually).
- Termly incident report received by e-Safety lead.
- Reporting to relevant Governors during committee meetings.
- Dialogue within the school community to ensure there is a good knowledge and understanding regarding E-safety.

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, although the day-to-day responsibility for E-Safety will be delegated to the E-Safety Lead.
- The Head teacher/Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable CPD opportunities to enable them to carry out their E-Safety roles and to train other colleagues, where relevant.
- The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to offer support to those colleagues who take on this role.
- The Head teacher and Deputy Head teacher are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

- The Head teacher, working alongside the E-Safety Lead, ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incidents.
- Regular monitoring of E-Safety incident logs by SLT (termly).

The E-Safety Lead:

- Takes day-to day-responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policy / documents.
- Working alongside the Head teacher, ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Undertakes training and provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school technical support staff (IT Assist).
- Receives reports of E-Safety incidents via SENSO (daily).
- Concerning incidents uploaded to CPOMS.
- E-Safety incident report to be created termly and presented at SLT meetings.
- Trends and concerns monitored and relevant training implemented.
- Meets with the E-Safety Governor to discuss current issues and review incident logs.

Teaching and Non-Teaching Staff:

- Have an up to date knowledge and awareness of online safety matters and the current policies and practices.
- They report any suspected misuse to the Head teacher or E-Safety Lead for investigation.
- To address online safety issues across the curriculum.
- E-Safety issues/trends in class to be addressed through teaching and learning.
- To monitor the use of digital technologies in their lessons.
- Where internet use is planned during lessons; it is best practice that children should be guided to sites which have been checked for suitability and processes are in place for dealing with any unsuitable material that might be found.

Children:

- Will be expected to know and adhere to the policies and procedures when using technology related to school based activities.
- Develop a good understanding of the importance of using good online safety practice at all times.
- In key stage 2, have a good understanding of research skills and the need to uphold copyright regulations.
- Recognise cyber bullying and know the procedures to report any incidents.
- Children to access the internet using their own login details.

Teaching and Learning

E-safety should be included in all areas of the curriculum, with key messages being constantly reinforced. Children need the help and support of the school to recognise and avoid any online safety risks and build their resilience. The E-Safety curriculum is broad and progressive, ensuring knowledge is relevant for all learners. There will be opportunities for it to be taught using some creative activities and will be provided in the following ways:

- A planned E-Safety curriculum delivered explicitly during computing and PSHE lessons and reinforced during the teaching within other subject areas.
- Staff acting as exemplary role models in their use of digital technologies, the internet and mobile devices.
- Important E-Safety messages reinforced in assemblies and across the curriculum when using or discussing technology.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content.
- Any serious content flagged by SENSO will be addressed at the earliest convenience.

Internet access

The Internet can be an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff, parents/carers and children, therefore the school has a duty to provide children with quality internet access as part of their learning experience:

- School internet access will be directed for children's use including appropriate content filtering.
- Children will be asked to log on to iPad devices or to use SENSO for internet browsing to maximise monitoring.
- Children will be given clear objectives for internet use and taught what is and is not acceptable.
- As part of the new computing curriculum, all year groups will experience E-Safety lessons and be regularly reminded about staying safe on the internet/on line. These lessons will include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of internet derived materials by staff and children complies with copyright law.

We ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of children to ensure inclusion for all and that all children are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEN Lead and individual teachers to ensure all children have equal access to success in this subject.

Authorised Internet Access

By explicitly authorising use of the school's internet access, children, staff, governors and parents are provided with information relating to E-Safety and agree to its use:

- The school will maintain a record of all staff and children who are granted internet access.
- All staff must read and sign the 'E-Safety Agreement' *(Appendix 2)* before using any school computing resource.
- Parents will be informed that children will be provided with supervised internet access and asked to sign and return a consent form for child access. *(Appendix 1)*

World Wide Web

The internet can open up new and fantastic learning opportunities and has become an essential part of the 21st century for children. Learning, homework and sharing through social media are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- SENSO will capture any inappropriate use of the internet.
- If staff or children discover unsuitable sites, the URL (address) should be reported to the Head teacher and CPOMs should be logged if a child has accessed inappropriate content.
- CPOM E-Safety concerns will be reviewed termly by the DSL and E-Safety Lead.
- The school will ensure that the use of internet derived materials by staff and children complies with copyright law.
- Children will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Children will be taught to be responsible when using the World Wide Web.
- The school will work in partnership with the Local Authority and IT Assist to ensure filtering systems are as effective as possible.

E-mail

E-mail is a quick and easy method of communication and ensuring beneficial and appropriate usage is an important part of E-Safety:

- Child access in school to external personal e-mail accounts is not allowed.
- E-mails sent to external organisations should be written in the same way as a letter written on school headed paper (i.e. appropriate vocabulary/formal style).
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding. If in doubt, IT Assist can support with this.
- Staff should always use their school e-mail account when communicating any school related business.
- Staff emails should not be given out by teachers to parents. Instead, the school's admin account should be used.

Social Networking *(Also see Social Media Policy)*

Social networking internet sites such as Facebook and Twitter provide facilities to chat and exchange information on the internet/online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- With the exception of Twitter, which is used by staff to communicate with parents, use of social networking sites in the school, is at present not allowed and will be blocked/filtered.
- Children will be advised never to give out personal details of any kind that may identify themselves, other children, their school or their location. This will also include not using personal photographs and videos.
- Children and parents will be advised that the use of teenage/adult social network spaces outside school (Facebook etc.) is inappropriate for primary aged children.
- Children will be encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- Parents, children, staff and governors must never discuss children, children's work, staff or the school on personal social networking sites. The governors may consider taking legal action, where appropriate, to protect children and staff against cyber bullying and defamatory comments.

- Children, staff and parents/carers will be given information about using privacy settings.
- Children, staff and parents/carers will be made aware that there is an option toreport misuse/abuse on social networking sites.

Cyberbullying

Cyberbullying will not be tolerated in our school as any kind of bullying is unacceptable (see our Anti-Bullying Policy). Any incidents of cyberbullying will be recorded in the E-Safety log and in the anti-bullying log (within CPoms) and the incident dealt with in line with our Anti-Bullying Policy.

Mobile Phones/Devices

Many mobile phones/devices have access to the internet and picture and video messaging, and these can present opportunities for unrestricted access to the internet and sharing of images. There are therefore risks of mobile bullying, or inappropriate contact.

- Children in Nursery – Year 5 **should not bring mobile phones** into school.
- Children in Year 6 (and Year 5 from Summer term) can, by permission of the Head teacher, bring mobile phones to school, where it is seen by the school and parents as a safety/precautionary use for children who are travelling to and from school without adult supervision. In these instances, children should hand their phones, at the start of the day, to the Year 5 and 6 class teacher, who will lock them away and hand them back at the end of the day; however, **school will not accept any responsibility for lost or damaged phones.**
- Parents will be required to given written permission before any child is permitted to bring their device to school.
- Children will be made aware that they are not allowed to take photographs/videos on their mobile devices anywhere on our school premises/grounds.
- The sending of abusive or inappropriate text messages is forbidden.
- Mobile devices with their own internet connectivity (mobile phones, tablets, iPads, handheld gaming units etc.) should not be brought into school for use by the children.
- Staff should always use a school phone to contact parents. Where this is not possible, staff must block their caller ID either within the phone or using 141.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom during lesson time (unless it is being used as a teaching resource).
- All staff and visitors should ensure that their phones are turned off/in silent mode and stored safely away during the teaching day.
- Staff must only use their mobile phones for personal use during break/ lunch period when no children are present.
- If parents/carers/family members take photographs or videos in assemblies, performances or on visits, these **must not** be distributed over social media sites (e.g. Facebook/Twitter/Instagram etc). If the school becomes aware that people have posted photos/videos from school related events on social media sites, then those responsible may be stopped from attending events or going on trips in the future.
- A teacher must request permission from the Headteacher to use their personal device for recording a class or school performance, this should only be permitted if school iPad quality or storage is compromised. Once recorded it must be immediately downloaded to the school drive and then deleted from the device.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Children will only use digital cameras or video equipment at school when specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Published Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by senior staff, with the understanding that images are strictly for personal use and not for publication in any manner.
- School staff will use school devices to take photographs/videos of any school related activities.
- A teacher must request permission from the Headteacher to use their personal device for recording a class or school performance, this should only be permitted if school iPad quality or storage is compromised. Once recorded it must be immediately downloaded to the school drive and then deleted from the device.
- Recordings of school related activities may be uploaded to Seesaw, Twitter or the school YouTube (private) – where parental permission has been given.

Video Conferencing/Skype/Zoom

Video conferencing may be undertaken by staff on occasions where this is a necessary part of the learning and will be done as a whole class activity, supervised by an adult at all times using either a teacher's laptop or iPad. IT Assist will need to be made aware of such plans to ensure filtering is not in place for the duration of the call. Video conferencing will be considered in the event of a school closure.

Seesaw Digital Learning Journals

Children have their own Seesaw digital learning journals which provides a powerful way of collating and celebrating achievements and sharing with our parents/carers. Children are able to post images, videos and audio recordings related to their classwork on their journals. All uploads, including comments, have to be approved by the class teacher.

Parents, via the Seesaw Family app and website, only have access to their own child's journal content. Parents sign a school Seesaw consent form before being provided access to their child's learning journal. (See Appendix 3). Seesaw is compliant with the GDPR in how it stores data.

In light of an event causing our school to close, remote learning will occur. Seesaw will be used in the first iinstance by teachers as a means to communicate and issue work electronically to children. Home Learning codes will be issued to children to ensure privacy and data protection for all when working remotely. Class login codes, which allow access to the whole class learning journal, are not to be sent home.

Staff are responsible for everything they send on Seesaw and must abide by the rules and stipulations within this document and Appendix 2. All educational links and resources sent to children should be checked and certified and all communication between children and staff should remain on the learning journal for future reference.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Members

of staff or children who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Published Content and the School Websites/Social Media Accounts *(also see Social Media Policy)*

The school website is a valuable source of information for the school community, governors, parents/carers and potential parents/carers.

- Contact details on the website will be the school address, e-mail and telephone number, as well as a contact person, e.g. the Head teacher and Admin Officer.
- Staff's personal information will not be published.
- Children's full names will not be published.
- The Head teacher and SLT will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Children's full names will not be used anywhere on the website or social media accounts, particularly in association with photographs.
- Consent from parents will be obtained before photographs of children are published on the school website or social media pages.

System Security

- The school computing system's capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and IT Assist.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available in line with data protection regulations and the school's data protection policy.

Assessing Risks

The school will take 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. The school does not accept liability for the material accessed, or any consequences of internet access. The school will audit computing use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Children and parents will be informed of the complaint's procedure.
- Discussions may be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Children:

- All children will be informed of the importance of being safe on the Internet, including social networking sites such as Facebook (objectives appropriate to age). This will be strongly reinforced across all year groups during computing lessons and all year groups will look at different areas of E-Safety during cross curricula lesson delivery.
- Children will be informed that internet use will be monitored and any misuse will be reported to the Head teacher and sanctions applied.

Staff:

- All staff will be given the Social Media and E-Safety Policies and will be required to sign the "Adults in School E-Safety Agreement" *(Appendix 2)*
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times (in line with Teacher Standards).

Parents/Carers:

Many parents/carers may have only limited understanding of E-Safety and the risks/issues and may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet – they may also be unaware of how to respond. The school will therefore seek to provide information and awareness through this policy by:

- Drawing attention to the School E-Safety Policy in newsletters and on the school website.
- Sending invitations to attend E-Safety chats/meetings and invitations to join children in E-Safety lessons.
- Sending information regarding keeping children safe and their hardware protected to all parents/carers
- Issuing parents with a list of helpful websites if they wish to access further information on E-Safety.

Review of policy

Due to the ever-changing nature of information and communication technologies, this policy is to be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies or new threats to E- Safety.

Appendix 1
Broadwood Primary School E-Safety Agreement
Children and Parents/Carers

Computing, including the Internet, email, mobile phones, iPads, tablets, digital cameras etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using technologies. Please discuss these rules with your child - the rules will help us to be fair to ourselves and others and keep everyone safe.

- I will only use the school's computers/mobile devices for school purposes.
- I will not give out my personal details e.g. name, phone number or address.
- Any messages I send will be responsible, polite and sensible.
- I will not arrange to meet anyone who I have only met on the Internet.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will turn off my iPad/close the laptop lid and tell my teacher immediately.
- I know that the school may check my computer files and monitor the internet sites I visit.
- I know that the school systems will take a screenshot of inappropriate content on my device.
- I know that if a member of the school staff is concerned about my E-Safety, my parent/carer may be contacted.
- I know that I am not allowed to bring my mobile phone into school unless I am in Year 6, or year 5 in Summer term only, and have received permission (on safety grounds for travelling to and from school without adult supervision) for me to do so. If I do receive permission, I understand that my phone will be handed in at the beginning of the school day and kept by my teacher until the end of the school day.
- I will only access my own Learning Journal on Seesaw and will not post as someone else or pose as another child on other software.
- I understand that if I do bring my phone onto the school premises, the school will not be liable if it is lost, stolen or damaged.
- I will not take photographs/videos on my mobile device anywhere on our school premises/grounds.
- I know that I am not allowed to bring devices with internet connectivity – i-pad, handheld consoles, tablet etc. into school.
- I understand that if I deliberately break these rules, I could be stopped from using the internet and/or computers in school and further action may be taken by the head teacher/senior management team. In the event of a serious incident, the matter may be referred to the police.

The full E-Safety Policy can be viewed on the school website https://www.broadwoodprimary.co.uk and/or if you would prefer to see a paper copy, then please ask at the school office.

Please read and sign the attached agreement to allow your child to access the Internet at school. Your son/daughter must also sign the agreement and it must be returned to class teachers as soon as possible.

Broadwood Primary School
E-Safety Agreement
Children and Parents/Carers

Child Name _____

Child's Agreement

I understand the Broadwood E-safety rules and I will use all computing devices and the internet in a responsible way and obey these rules at all times.

Child please sign here ……Date……
Please print name here ……..

Parent/Carer's Consent for Internet Access

I have read and understood the school's E-safety agreement and give permission for my child/children to access the internet. I understand that Broadwood Primary School will take all reasonable precautions to ensure children cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the internet facilities. I understand that if, after seeking permission, my Year 6 child is allowed to bring a mobile phone to school, the school will not be responsible if the device is lost, stolen or damaged.

Parent/Carer please sign here …… Date……

Please print name here ……..

Parent/Carer's Consent for Web Publication of Work

I agree that, if selected, my child's/children's work may be published on Broadwood Primary School's website or on a teacher affiliated Twitter account.

Parent/Carer please sign here …… Date……

Please print name here ……..

Parent/Carer's Consent for Web Publication of Photographs

I agree that photographs that include my child/children may be published on Broadwood Primary School's websites or on a teacher affiliated Twitter account, subject to the school rules that photographs will not clearly identify individuals by full names.

Parent/Carer please sign here …… Date……

Please print name here ……..

Parent/Carer's Use of cameras/mobile devices in and around school

I understand that if I take photographs/videos in school assemblies/performances or on visits, these **must not** be distributed over social media sites (e.g. Facebook/Twitter/Instagram etc). If the school becomes aware that I have posted photos/videos from school related events on social media sites, then I understand that I may be stopped from attending events or going o trips in the future.

Parent/Carer please sign here …… Date……

Please print name here ……..

Appendix 2
Broadwood Primary School E-Safety Agreement
Adults in School

Computing and the related technologies such as email, the Internet, iPads and mobile phones/devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of digital technology.
All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher and/or school E-Safety Lead.

- I will support and promote the school's E-Safety Policy and help children to be safe and responsible in their use of Computing and related technologies.
- I will only use the school's e-mail / internet / intranet / learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher or Governing Body.
- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that my passwords are secure and robust.
- I will only communicate with parents using the school admin email account, Seesaw or the school phone. Where this is not possible (i.e. COVID19), I will abide by the guidance within this document.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately in line with GDPR and the schools Data Protection Policy.
- I will not browse, download or upload material that could be considered offensive or illegal.
- Images of children will only be taken and used for professional purposes in school and will not be distributed without consent of the parent/ carer.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head teacher.
- I understand that I am not permitted to use my mobile phone within the classroom during lesson time (unless it is being used as a teaching resource). I will ensure that my phone is turned off/in silent mode and stored safely away during lesson time, unless special permission has been granted by the Head teacher.
- I understand that I may use my mobile phone in the staffroom or classroom during the break/ lunch period, however I know that phones should not be accessed in corridors and/or when children are in the vicinity.
- I will ensure that any social media accounts that I have (Twitter, Facebook etc.) have privacy setting set appropriately and do not compromise my professional position. I understand that it is inappropriate to discuss any aspect of my involvement with Broadwood Primary School on social networking sites. I understand that I should not discuss children, children's work, staff, or any aspect of school life. I also understand that I should not place any images relating to Broadwood Primary School, its staff, children or children's work on social networking sites with the exception of my own professional Twitter account.
- I will not under any circumstances accept friend requests from a person I believe to be a current attendee, or past attendee under the age of 18 at Broadwood Primary School.
- I will not communicate with parents / children using DM on Twitter or other social media platforms. All contact on Twitter will remain in the public forum.
- I will respect copyright and intellectual property rights.

I agree to follow this code of conduct and to support the safe use of Computing throughout the school.
The full E-safety policy and Social Media Policy can be viewed on the school website - www.broadwood.newcastle.sch.uk and is also available in electronic and paper form, in line with school protocol. Failure to adhere to this agreement may result in disciplinary action and in serious cases may be referred to the police.

Please sign here……..Date……..

Please print name here……

Role in school……

Appendix 3
Broadwood Primary School Seesaw Consent Form

At Broadwood Primary School, we are continually looking at ways to make learning more accessible and engaging for our children, and one of the ways in which we would like to do this is through the use of technology in class. When using technology, it can be difficult to capture the work children do, therefore we would like to set up accounts for our children using an app called Seesaw.

Seesaw (http://seesaw.me), is a secure online journal where students can document and reflect on what they are learning in class and your child will be able to add the things we work on (including photos, videos, worksheets, drawings and voice recordings) to their Seesaw journal.

In order for your child to use Seesaw, the app requires your child's name in order to be able to associate work like their photos, videos or voice recordings with their account. Seesaw only uses this information to provide the service and doesn't advertise in Seesaw, create profiles of students, or share or sell your child's personal information or journal content. It only adds their name to the teachers' class list. You can read more about their strong privacy promises here: https://web.seesaw.me/privacy.

Under an EU law called the General Data Protection Regulation (GDPR), in order for your child to use Seesaw, we must have the consent of the parent or carer.

As a school, we are incredibly excited by the opportunities Seesaw will provide, and its use will help us to continue to make the curriculum more exciting and engaging.

Please sign below and return this permission slip so that your child can access and use Seesaw in class and for homework activities.

_____

I give consent for my child, listed below, to use Seesaw for class and homework activities.

Student Name: ……_____

Parent Printed Name: ……

Parent Signature: ……

Date: _____