

Broadwood Primary School



ONLINE SAFETY POLICY

Last reviewed	June 2026
Reviewed by	Curriculum Committee
Next review date	June 2027

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 Online Safety?

Online safety (eSafety) involves protecting personal information, devices, and well-being from digital risks like scams, harassment, and inappropriate content.

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.

Introduction

This Online Safety Policy sets out Broadwood Primary's commitment to providing a safe, inclusive, and empowering digital environment for all pupils. The policy is designed to ensure compliance with the 2014 National Curriculum for Computing and statutory safeguarding requirements. It outlines our whole-school approach to teaching online safety, embedding it across the curriculum and wider school life, and ensuring all staff, pupils, and parents are equipped to identify, manage, and respond to online risks.

Aims

- Equip pupils with the knowledge, skills, and attitudes to use technology safely, respectfully, and responsibly.
- Enable pupils to recognise, assess, and respond to online risks, including cyberbullying, online abuse, radicalisation, exploitation, and privacy breaches.
- Foster a culture where pupils feel confident to report concerns and seek help regarding online behaviour.
- Ensure all staff are trained and confident in delivering online safety education and responding to incidents.
- Engage parents and carers in supporting online safety at home and in school.
- Ensure online safety education is accessible, inclusive, and responsive to the needs of all pupils, including those with SEND and EAL.
- Regularly review and adapt provision to address emerging technologies and risks.

Statutory Requirements

- Deliver online safety education as part of a broad and balanced curriculum (Keeping Children Safe in Education).
- Teach pupils to use technology safely and respectfully, keep personal information private, and know where to seek help (2014 National Curriculum for Computing).
- Provide Relationships Education, including online relationships and behaviour (Children and Social Work Act 2017).
- Safeguard and promote the welfare of pupils, including protection from online harm (Education Act 2002).

- Ensure accessibility and inclusion for all pupils, including those with SEND (Equality Act 2010; SEND Code of Practice 2015).
- Educate pupils about personal data privacy and the risks of sharing information online (Data Protection Act 2018/GDPR).
- Prevent online radicalisation and extremism (Prevent Duty, Counter-Terrorism and Security Act 2015).
- Maintain appropriate filtering and monitoring systems to protect pupils online (KCSIE).

Roles and Responsibilities

Role	Responsibilities
Headteacher	Overall responsibility for safeguarding, policy implementation, and staff training.
Online Safety Lead	Curriculum planning, monitoring provision, staff support, incident management, and policy review.
Designated Safeguarding Lead (DSL)	Oversight of safeguarding records, online incident response, and training.
Class Teachers	Deliver online safety education, model safe online behaviour, and report concerns.
Support Staff	Support delivery, reinforce messages, and report concerns.
Governors	Monitor policy effectiveness, ensure statutory compliance, and support strategic development.
Pupils	Engage with online safety education, follow school rules, and report concerns.
Parents/Carers	Support online safety at home, engage with school initiatives, and reinforce safe behaviour.

Curriculum Coverage

- Understanding how to use technology safely, respectfully, and responsibly.
- Recognising acceptable and unacceptable online behaviour.
- Identifying risks associated with online activity, including cyberbullying, privacy, digital footprint, and misinformation.
- Knowing how and where to report concerns about content, contact, or conduct online.
- Exploring the opportunities and challenges of online communication and collaboration.
- Developing critical thinking skills to evaluate online information and recognise potential harm.
- Understanding the importance of personal data privacy and strategies for protecting personal information.
- Awareness of online radicalisation, grooming, and exploitation, and strategies for staying safe.
- Building resilience to peer pressure and inappropriate online influences.
- Promoting positive online relationships and respectful digital communication.

Curriculum Implementation

- Online safety is embedded across the curriculum, including Computing, PSHE, Relationships Education, and other relevant subjects.
- The curriculum is mapped to ensure age-appropriate progression from basic awareness in early years to more sophisticated understanding in upper primary.
- Teaching approaches include:
 - Scenario-based learning, role-play, and real-life case studies.
 - Class discussions, group work, and critical thinking activities.
 - Use of Seesaw to evidence learning.
 - Peer-led initiatives and pupil voice activities.
- Regular review and adaptation of curriculum content to address emerging risks and technologies.
- Use of high-quality, up-to-date resources, including those from recognised online safety organisations.
- Structured opportunities for parental engagement, including workshops, newsletters, and online resources.
- Differentiated teaching and resources to ensure accessibility for all pupils, including those with SEND and EAL.

Assessment

- Ongoing formative assessment through observation, questioning, discussion, and scenario-based activities.
- Summative assessment using:
 - Pupil self-reflection and peer assessment.
 - Teacher judgement based on evidence in pupil work (e.g., posters, picture evidence on Seesaw).
 - Pupil surveys and feedback to gauge understanding and attitudes.

Inclusion

- Online safety education is differentiated to meet the needs of all learners, including those with SEND and EAL.
- Adapted resources, visual supports, and additional adult support are provided as required.
- Lessons are designed to be accessible, engaging, and relevant to pupils' experiences and backgrounds.
- Pupil voice is actively sought to ensure content is meaningful and inclusive.
- Regular review of provision to address barriers to participation and understanding.

Professional Development

- All staff receive regular, high-quality training on online safety risks, curriculum content, and safeguarding procedures.
- Training is updated in response to emerging risks or incidents.

- Staff are supported to develop confidence in delivering online safety education through peer support, coaching, and access to specialist resources.
- Opportunities for staff to share best practice and reflect on provision are embedded in school routines.

Seesaw Digital Learning Journals

- Children have their own Seesaw digital learning journals which provides a powerful way of collating and celebrating achievements whilst 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. Any parent comments on posts are approved by class teachers and any inappropriate comments are passed to the Safeguarding team to review and address. Equally, pictures and text can be sent by parents through the messaging services, these cannot be seen by pupils. Communication through the messaging service can be viewed by all staff members using Seesaw. 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 using Seesaw. Seesaw will be used in the first instance 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. 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.

Mobile Phone Use

The use of mobile phones to take photographs, record videos, or access the internet without permission is strictly prohibited. Any misuse of mobile devices will be addressed in line with the school's behaviour, safeguarding, and online safety policies. For pupils this may result in parents or carers being contacted and appropriate sanctions being applied.

- 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 teachers, who will lock them away and hand them back at the end of the day. School will not accept any responsibility for lost or damaged phones.
- Parents will be required to give 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.

- 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 and permission has been granted by the Headteacher).
- All staff and visitors should ensure that their phones are on 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 to record 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.

Monitoring Children's Online Use

The school uses Senso app to monitor and safeguard pupils' online activity when accessing the internet on school devices and networks. Senso helps ensure that children use technology safely and appropriately by monitoring online searches, websites visited, and other digital activity in line with the school's acceptable use expectations. If concerning, unsafe, or inappropriate behaviour is identified, the system automatically alerts the Designated Safeguarding Lead (DSL) and relevant staff so that concerns can be reviewed promptly and appropriate action can be taken to support and protect pupils. The safeguarding team reviews trends in violations and determines any appropriate follow-up action, which may include discussions with pupils, targeted online safety lessons and support to address identified concerns and reinforce safe online behaviour. Monitoring is carried out in accordance with safeguarding responsibilities, data protection requirements, and the school's commitment to promoting safe and responsible use of technology.

Monitoring and Review of this policy

- The Online Safety Policy is reviewed annually, or in response to significant incidents or changes in statutory guidance.
- Monitoring includes:
 - Lesson observations and curriculum audits.
 - Pupil, staff, and parent surveys and feedback.
 - Review of safeguarding and incident records.
 - Evaluation of assessment outcomes and evidence of impact.
- The Online Safety Lead reports regularly to the Headteacher and Governors on policy implementation and effectiveness.
- Pupil voice and parental feedback are used to inform ongoing development.

Appendix 1

Broadwood Primary School Online 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 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 know that if a member of the school staff is concerned about my Online 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 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 Online 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.

Online safety Agreement - Children and Parents/Carers

Child Name _____

Child's Agreement

I understand the Broadwood Online 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 hereDate.....

Parent/Carer's Consent for Internet Access

I have read and understood the school's Online 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.....

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 the school's social media accounts:

Parent/Carer please sign here Date.....

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 the school's social media accounts, subject to the school rules that photographs will not clearly identify individuals by full names.

Parent/Carer please sign here Date.....

Parent/Carer's Consent for Child's use of Seesaw

I agree that my child can use Seesaw for learning purposes. I am aware that if I sign up to the Family Seesaw App, that I will be able to view all posts on my child's account.

Parent/Carer please sign here Date.....

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 sites, then I understand that I may be stopped from attending events or going on trips in the future.

Parent/Carer please sign here Date.....

Appendix 2

Broadwood Primary School Online 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 Online safety Lead.

- I will support and promote the school's Online Safety Policy and help children to be safe and responsible in their use of technologies.
- I will only use the school's e-mail / internet / 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 my use of the internet and other related technologies is 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 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 refrain from accepting social media friend requests from family members of pupils in school.
- Where I am already a friend of a family member prior to a pupil attending Broadwood, I will remove them in order to maintain professional boundaries, protect privacy, and avoid conflicts of interest until that child is no longer at our school.
- I will not communicate with parents/families or children on social media platforms.
- I will respect copyright and intellectual property rights.

I agree to follow this code of conduct and to support the safe use of technologies throughout the school. 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.....