Brunshaw Primary School

'Inspiring children to be resilient and aspirational learners, within a positive and considerate community.'

Online Safety Policy

September 2025

Agreed by Governors:

Overview
The purpose of this policy is to safeguard and protect all members of Brunshaw Primary School's community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of our school. This includes staff, students, pupils, volunteers, parents/carers, visitors and community users who have access to and are users of Brunshaw's digital technology systems, both internally and externally.

This policy has been written by the school, building on government guidance; it operates in conjunction with other policies including those for Computing, Positive Relationships & Behaviour and Safeguarding & Child Protection. The school's Designated Safeguarding Lead (DSL) takes overall responsibility for online safety at school.

School Statement
Brunshaw Primary School affirms that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

At Brunshaw, we recognise that the internet and associated devices are an integral part of everyday life, used for education, business and social interaction. Use of the internet and other technologies is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use a variety of technology widely outside school and need to learn how to evaluate information and to take care of their own safety and security. As such, the school has a duty to empower all learners to build resilience and to develop strategies to recognise and respond to online risks.

The school's internet access is designed expressly to support and enhance education and includes filtering and monitoring systems appropriate for all users. Pupils will be taught what types of internet use are and are not acceptable, and will be given clear objectives for lessons involving internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Prevent
As part of our ongoing commitment to safeguarding at Brunshaw, all staff members have received PREVENT training from the local authority's Prevent Team, which is refreshed every 18 months – 2 years, whilst the online training is completed annually. As a school, we utilise the local authority's Prevent Audit & Planning tool to share roles and responsibilities with all staff and consistently monitor the efficiency of our Prevent procedures, to ensure the safety of all in our school community. Brunshaw Primary School employs monitoring and filtering systems, as well as a firewall, which prevents any staff/student/visitor from accessing extremist websites and material.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information used and to respect copyright when using material from the internet in their own work.

Staff and governors

All staff and governors are required to annually sign and adhere to the Staff Acceptable Use Policy before accessing school technology. All staff will be expected to read the Online Safety and Social Networking Policies as part of induction, and then annually (or when updates are made) as part of the school's Safeguarding training. Staff members have personal logins to school computers and are aware that internet use is monitored and can be traced to the individual user. Discretion and professional conduct are essential. Staff training in safe and responsible internet use will be provided as required.

Parents/Carers

Parents/carers will be signposted to the Online Safety and Pupil Acceptable Use Policies on the school website at regular intervals throughout the school year. The school website contains safe search website links for children to conduct digital research at home and online safety updates are included in our weekly school newsletter. Online safety issues in school will be handled sensitively, and parents/carers will be advised accordingly.

The school office will contact parents/carers via text message, Class Dojo and/or email when the need occurs e.g. school closures, cancellation of after school activities, reminders about meetings and events etc. Parents should not contact staff through text messaging or by using the Messages function of Class Dojo.

Pupils

All pupils must understand and sign the Pupil Acceptable Use Policy at the start of each school year. This is then displayed in the classroom and referred to regularly. Pupils understand the consequences which may result if this policy is violated. Pupils are regularly shown the child-friendly version of the Online Safety Policy and know where they can find this on the school website. KS2 pupils have personal logins to the school computers, whilst KS1 pupils use a class login account. All pupil iPads are numbered and each class has a list, assigning a specific iPad to each child. This allows all iPad use to be monitored and any pupils using an iPad inappropriately can be identified.

Security, filtering and monitoring

The capacity and security of the school's ICT systems will be reviewed and monitored regularly with the ICT technician, Online Safety Lead, governors and DSL. Virus protection will be updated regularly as required. The provision of filtering and monitoring will be reviewed at least annually by governors to ensure it continues to meet the needs of pupils and staff and reflects the school's specific use of technology. Important findings and any concerns will be reported to the DSL. Reports of suspicious internet searches are provided weekly to the ICT technician and shared with the DSL and Online Safety Lead as required. Filtering systems allow

the ICT technician to identify individuals (both staff and pupils) attempting to access unsuitable material using a school laptop. Brunshaw Primary School uses the On Guard software on all laptops. This software is designed to check everything that gets typed into any computer, no matter what the program is, in real time. Using its own Artificial Intelligence, it decides if it needs to be looked at and takes a screenshot of what was written to pass on to a member of the Senior Leadership Team for further investigation.

The school will work with the local authority and Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the head teacher, ICT technician, Online Safety Lead and logged via CPOMS. All staff know how to report and record their concerns in this way. All CPOMS entries regarding Online Safety incidents are discussed termly by the school's staff and governor Online Safety Group. This enables school to identify issues concerning internet access and put interventions in place. Any material that the school believes is inappropriate will be reported to appropriate agencies.

Published content including pupil images

Contact details on the website/social media pages are the school address, e-mail and telephone number. Staff, governor or pupils' personal information will not be published. The head teacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website/social media pages or in association with photographs. Written permission from parents/carers will be obtained on the pupil's entry to school, with separate choices for all platforms (e.g. photograph allowed on newsletter but not social media). Parents/carers will be notified at all public performances about the guidelines for confidential use of images in respect of social networking sites.

The school will block/filter access to social networking sites. Through online safety lessons, pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents/carers will be advised that the minimum age in the UK for children to access social media platforms, such as Facebook, TikTok, WhatsApp and SnapChat, is 13. They will also be offered guidance through workshops, events and newsletters on how they can best keep their children safe whilst using the internet at home.

Artificial intelligence (AI)

At Brunshaw Primary School, we are aware that our pupils are growing up in a world increasingly driven by Artificial Intelligence (AI). Pupils are taught about the potential dangers of AI as part of Online Safety and PSHE lessons. These sessions include ways for children to evaluate the authenticity of websites, images and videos, as well as conversations they may have with others over the internet. Due to the potential exposure to inappropriate content, children are not allowed to use AI at school whilst

using school devices. Staff will respond appropriately to changes in the National Curriculum and other statutory guidance in regards to the use of AI in the classroom.

Staff are aware of the opportunities that AI offers with regards to reducing teacher workload and producing bespoke teaching and learning resources. Staff understand that AI should not be used as a replacement for their knowledge as a teacher, be over-relied upon, or used to upload documents containing personal information of any staff members or pupils. Staff do not use AI in view of pupils (for example, on their interactive whiteboards) due to the potential for inappropriate search results to be displayed. Methods on the best use of AI to support teaching and learning are shared regularly with staff by the Computing & Online Safety Subject lead and IT Technician.

Video conferencing

Video conferencing should use the educational broadband network, where possible, to ensure quality of service and security rather than the internet. Pupils are not permitted to engage in video conferencing outside of a planned lesson and under the supervision of staff. Video conferencing will be appropriately supervised for the pupils' age. If staff and pupils are using video conferencing remotely, the conduct of all participants must be the same as that expected in school. Where possible, pupils should engage in video conferencing in a communal area of the home with a parent/carer present in the room.

Mobile phones, emerging and wearable technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones should not be brought into school by pupils and will not be used during lessons or school time. If mobile phones need to be in school, e.g. for children walking home, they must be handed to the office at the start of the school day. If found during the school day, mobile phones belonging to pupils will be handed to the head teacher and parents will be contacted. All staff, parents and pupils are required to follow our policy for mobile phones in school.

Similarly, the use of wearable technologies (including smart watches and Fitbits) is not allowed by pupils in school. Aside from the expense and distress should such an item be lost or damaged, these devices are constantly evolving and present a risk to online safety. In exceptional circumstances, such devices must be handed into the school office at the start of the school day.

Online safety teaching and learning

Online safety teaching and learning at Brunshaw is school-wide and tailored to fit the needs and concerns of our pupils. We consistently aim to raise the profile of online safety for all stakeholders. This is achieved by:

- The Pupil Acceptable Use Policy is shared at the start of each school year. Pupils are required to understand and sign the policy before using technology and the consequences of non-compliance will be explained. A copy of the policy is displayed in all classrooms and referred to regularly.

- The Online Safety Champions. This group consists of a pupil representative from each class (Years 1-6), who meet with the Online Safety Lead each half term to share their thoughts, experiences and those of their class. The group act as ambassadors for online safety and lead events in school that support and develop our pupils' understanding of online safety.
- The Online Safety Group. This group consists of staff and governors and meets termly to discuss the feedback of the Online Safety Champions, efficiency of the school's filtering and monitoring systems, and any recorded online safety incidents logged via CPOMS.
- Use of the Education for a Connected World framework and Project Evolve resources for teaching Online Safety. Each half-term, teachers will use the Project Evolve Knowledge Map tool to assess the needs of their class in their assigned Online Safety stand for that half term. Teachers will use the results to target gaps in pupils' knowledge, by embedding online safety objectives into Computing lessons, and/or teaching them discretely.
- Three key online safety weeks throughout the year. The Education for a Connected World strands of 'Self-image and Identity' and 'Online Bullying' will be taught during the first week of the Autumn term and during Anti-Bullying Week in November, respectively. The whole school will also participate in the UK Safer Internet Centre's annual Safer Internet Day in February.

Assessing risks

The school will take all reasonable precautions to ensure that users are safe and access only appropriate material, and there is appropriate and substantial filtering and monitoring software in place to ensure that pupils do not access material linked to terrorism, extremism or of a sexual nature. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor local authority can accept liability for the material accessed, or any consequences of internet access. We will work with parents to support in the use of technology at home and we provide weekly updates through newsletters regarding popular sites and apps children are using.

The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

The Department for Education's Keeping Children Safe in Education 2024 states: "Abuse can take place wholly online, or technology may be used to facilitate offline abuse." Staff and governors will continue to have regular Safeguarding and Online Safety training. The guidance also explains that child-on-child abuse is most likely to include behaviours including cyberbullying and youth produced sexual imagery. Specific types of abuse may also include an online element, which may facilitate, threaten and/or encourage abuse and/or violence. Staff are aware of the potential

risks in regard to child-on-child abuse and understand how to record and handle any incidents, in accordance with school policy.

The Ofsted School Inspection Handbook 2024 states: "Inspectors will expect schools to assume that sexual harassment, online sexual abuse and sexual violence are happening in the community, and potentially in the school, even when there are no specific reports, and put in place a whole-school approach to address them" To ensure incidents of this nature are recognised and reported promptly, all staff at Brunshaw receive regular training on how to handle disclosures and log concerns on CPOMS. It is the responsibility of all staff within our school community to safeguard children, so all staff remain vigilant to the signs of abuse.

Reporting incidents

Any concerns or incidents regarding online safety are logged on CPOMS under the Online Safety category. These include any discussions with pupils regarding apps, devices, games and websites that they have viewed at home This is then immediately received by the SLT, DSL, Deputy DSLs and Online Safety Lead, as well as other key staff members relating to the child(ren) involved. All staff members are trained in how to do this and receive updates as part of Safeguarding and Online Safety training.
These incident reports are then used to inform the actions of the staff and governor Online Safety Group, direct the work of the Online Safety Champions and implement changes to the Online Safety curriculum if required.

Handling 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 safeguarding/child protection nature must be dealt with in accordance with school safeguarding/child protection procedures. Parents and pupils will need to work in partnership with staff to resolve issues.

Monitoring

All online safety incidents from the term are discussed in the staff and governor Online Safety Group meetings. Intervention and support will be planned in these meetings to support individual/groups of pupils and their families. Online Safety teaching and learning is monitored throughout the year, including as part of Computing, PSHE and RSE subject monitoring and to measure the impact of events such as visitors and Safer Internet Day.

Reviewed: June 2025
Next Review: June 2026