

Brunshaw Primary School



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

Online Safety Policy

September 2026

Agreed by Governors: 15/10/26

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, supported by government guidance. It operates in conjunction with other policies including those for Computing, PHSE, Mobile Phones in School, Acceptable Use of Technology and the Internet, 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 users 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.

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 related 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 devices and are aware that internet use is monitored and can be traced to the individual user. Discretion and professional conduct are essential. Staff receive online safety training and updates as required, and at least annually.

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 laptops and 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.

Parents/Carers

At Brunshaw, we recognise that parents and carers play a vital role in shaping children's early online experiences and in developing their understanding of, and positive attitudes towards, the online world. We work in partnership with parents and carers to equip our pupils with the skills, knowledge and understanding they need to access and use the internet safely, both in and out of school.

We support parents and carers in a variety of ways. They are regularly signposted to the school's relevant policies on the school website. The website also provides links to safe search sites that children can use when using the internet home. Online safety updates and relevant information are shared with parents and carers through the school newsletter and Class Dojo as required.

Any online safety issues that arise in school are dealt with sensitively, and parents and carers are informed and advised appropriately. Each academic year, parents and carers are given opportunities to come into school to receive further information and guidance on online safety issues that have been identified (by school or from parental feedback) as areas where additional support or understanding would be beneficial. These may include topics such as social media, artificial intelligence (AI) and appropriate levels of screen time. Sessions may take the form of assemblies, stay-and-learn activities with their children, or parent-only workshops, and are delivered by school staff and/or industry professionals. We welcome parental feedback about areas where they would value further support and use this to help inform future online safety sessions.

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, social media or by using the Chats function of Class Dojo.

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 and create a whole-school ethos of safe and responsible Internet use. 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 Pupil AI and Online Safety Policies are shared throughout each school year and are available on the school website.
- 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 discuss online safety concerns and important themes. The group act as ambassadors for online safety and lead discussions and 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, proficiency 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. Online Safety is embedded into our curriculum via Computing and PSHE lessons, as well as discrete Online Safety sessions. Coverage of the Education for a Connected World framework through use of the Project Evolve resources is mapped out for each year group.
- 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.
- Age-appropriate sessions at least annually for pupils and parents on topics including social media, AI and keeping personal information safe.
- Online Safety teaching and learning is monitored throughout the year, including as part of Computing, Online Safety and PSHE subject monitoring. Monitoring takes place through a variety of ways, including analysis of any online safety incidents, discussions with staff, pupils and parents and lesson observations. Monitoring findings are used to further develop and improve the online safety provision at Brunshaw.

Prevent

As part of our ongoing commitment to safeguarding at Brunshaw, all staff members have received Prevent training. Training is refreshed in line with statutory safeguarding requirements. 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.

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 risks of AI as part of Computing, Online Safety and PSHE lessons. These lessons include ways for children to evaluate the authenticity of online content, as well as conversations they may have with others over the internet. As the statutory primary National Curriculum does not require children to use AI, and due to the potential exposure to inappropriate content, children are not permitted or directed to use AI at school. 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 Lead and IT Technician. Further information on AI use at Brunshaw can be found in our separate AI policies for staff and pupils.

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. Permission for photographs to be shared is obtained from parents/carers on pupils' admission to school. Parents/carers will be notified at all school events that photographs and videos should not be taken. Images and videos of assemblies and performances will be taken by staff and made available to parents via appropriate means, such as Class Dojo and the school newsletter.

Video conferencing

Video conferencing should use the school's network, where possible, to ensure quality of service and security. Pupils are not permitted to engage in video conferencing outside of a planned lesson and under the supervision of staff. 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.

Pupils should not bring mobile phones onto the school site unless there are exceptional circumstances agreed in advance by the Headteacher. Where it is necessary for a pupil to bring a mobile phone to school (for example due to travel arrangements), the phone must be switched off on arrival and handed to the class teacher or school office for secure storage during the school day. Any mobile phone or smart device used in breach of policy will be confiscated. Further information on Mobile Phones in School can be found in our dedicated policy.

Similarly, the use of wearable technologies (including smart watches) 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.

Filtering and monitoring

The school's provision for filtering and monitoring is reviewed at least termly in meetings held between the ICT Technician, Online Safety Lead, relevant governors and DSL. Filtering systems allow the ICT technician to identify individuals (both staff and pupils) attempting to access unsuitable material using the schools network. Brunshaw Primary School uses the On Guard software on all individual login accounts. This software is designed to check everything that gets typed into the device, no matter what the program is, in real time. Using its own artificial intelligence, On Guard evaluates the need for review and sends a screenshot of what was typed to the Senior Leadership Team for further investigation. The use of On Guard software is described in the Acceptable Use Policies for both staff and pupils.

The school works with the local authority and Internet Service Provider to ensure systems to protect pupils are reviewed and improved. 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. 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, and recording concerns via CPOMS is covered in annual safeguarding training, as well as induction for new staff. Online safety incidents are quickly responded to swiftly with appropriate actions. Depending on the incident, these may include pastoral and/or educational responses and support for families.

Reviewed: September 2026
Next Review: September 2027