



Online Safety Policy

Policy Reviewed **March 2026**

Signed on behalf of Governing Body

To be next Reviewed **March 2028**

Online Safety Policy

Brushwood Junior School believe that online safety is an essential part of safeguarding and we acknowledge it is our duty to ensure that all pupils and staff are protected from potential harm online. We know that the internet and associated devices such as laptops, tablets, mobile phones and games consoles are an important part of everyday life. Brushwood empowers pupils to build resilience and develop strategies to manage and respond to risk online.

This Policy also relates to:

- Anti-Bullying Policy
- Child Protection Policy
- Keeping Children Safe in Education Sept 2023
- Attendance Policy
- Staff Code of Conduct
- SEN and Inclusion Policy
- Behaviour and discipline safety Policy
- Equal opportunities Policy
- RSHE Policy

The Governing Body reviews this policy bi-annually. The Governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the Governing Body receives recommendations on how the policy might be improved.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

[Teaching online safety in schools](#)

[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

[Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

At Brushwood Junior School we aim to:

- Have clear and robust processes in place to ensure the online safety of pupils, staff and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate incidents, where appropriate

The four key categories of risk

Brushwood's approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Filtering and monitoring

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system.

- **Filtering systems:** block access to harmful sites and content.
- **Monitoring systems:** identify when a user accesses or searches for certain types of harmful content on school and college devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content so they can intervene and respond.

The school recognises that no filtering and monitoring system is 100% effective, so use it alongside its existing safeguarding systems and procedures.

Designated Safeguarding Leads (Jo Robertson, Kirsty Haines and Emily Stevens) are responsible for monitoring the filtering reports daily. They monitor whether user access has been granted or denied to flagged sites or platforms and check under search terms for anything inappropriate that may be flagged. DSLs follow up every case where a user is found to be using inappropriate search terms or attempting to access unsuitable content. In the case of children, parents will be alerted. In the case of staff, this may result in disciplinary action.

Roles and responsibilities

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher and Senior Leadership Team to account for its implementation. The Governing Body will coordinate regular meetings with the appropriate staff to discuss online safety and review monitoring records provided by the Technical Support Provider, or online safety reports from CPOMS as provided by the Designated Safeguarding Lead (DSL).

Governors will:

- Ensure they have read and understood this policy
- Agree and adhere to the terms on acceptable use of Brushwood's ICT systems and the internet (appendix A)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable pupils, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Senior Leadership Team will:

- Ensure that staff have understood this policy, and that it is being implemented consistently throughout the school
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and acceptable use policy

- Work alongside the technical support provider to monitor the safety and security of school systems and networks
- Ensure online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Ensure there are robust reporting systems in place
- Ensure that appropriate risk assessments are undertaken regarding safe use of technology

Designated Safeguarding leads will:

- Support the staff to address any online safety issues or incidents
- Manage all online safety issues or incidents in line with the Child Protection policy
- Ensure all online safety incidents, including cyber bullying, are recorded on CPOMS and are dealt with appropriately
- Alert parents if their child has made an inappropriate search or attempt to access unsuitable content
- Update and deliver staff training on online safety, when necessary
- Liaise with other agencies and/or external services if necessary

The technical support provider will:

- Ensure there is an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact while at school, including terrorist and extremist material
- Ensure all ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the ICT systems monthly
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure that the technical infrastructure is secure and is not open to misuse or malicious attack

Online Safety Coordinator/Computing Lead will:

- Take the lead on online safety issues such as Safer Internet Day
- Review online safety policies and procedures
- Provide training and advice for staff
- Updates the online safety governor regularly
- Reports issues to the Senior Leadership Team
- Ensure users only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

All Staff will:

- Maintain an understanding of this policy
- Implement this policy consistently
- Adhere to cyber security expectations and protocols
- Agree and adhere to the terms on acceptable use of ICT systems and the internet (appendix A)
- Monitor pupil usage of computers, particularly when using the internet
- Record any online safety, including cyber bullying, incidents on CPOMS
- Respond appropriately to all reports and concerns about sexual harassment and/or violence, both online and offline and maintain an attitude of 'it could happen here'
- All digital communications with pupils/parents/carers is professional and only carried out using official school systems
- Online safety aspects are embedded across the curriculum
- Pre-plan internet sites so that they are suitable

Parents/Carers will follow guidelines on the appropriate use of:

- Digital and video images taken at school events

- Pupil's personal devices in school (named and stored in a locked safety box in the classroom)
- Aware of the age limits of popular social media networking sites

Pupils will:

- Agree and adhere to the terms on acceptable use of ICT systems and the internet (appendix B)
- Take responsibility for using the devices in accordance with the Pupils Acceptable Use Agreement
- Have a good understanding of research skills
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understand the use of mobile phones including the policy on taking/using images and on cyber bullying

Vulnerable pupils

We are aware that pupils are more vulnerable online due to a range of factors. This may include, but is not limited to, pupils in care, pupils with Special Educational Needs/Disabilities (SEND) or mental health needs, pupils with English as an additional language (EAL) and pupils experiencing trauma or loss. Brushwood will ensure that there is differentiated and ability appropriate online safety of education which is accessible to vulnerable pupils and they are supported, if necessary.

Staff using work devices outside school will:

- Ensure the device is password protected using strong passwords which are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters
- Ensure devices are automatically locked if left inactive for a period of time
- Not share the device among family or friends
- Will not install any inappropriate software including spyware
- Keep operating systems up to date and will always install the latest updates
- Not use the device in any way that would violate the terms of acceptable use

Educating pupils about online safety

Online safety is taught as part of the curriculum and is revisited at least every half term. Brushwood follows the [National Curriculum Computing programmes of study](#). We update our curriculum regularly to incorporate any changes or updates with online safety in order to keep the pupils safe.

By end of Key Stage Two, all pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Educating parents about online safety

Parents/Carers play an essential role in the education of their children and in monitoring/regulation of their child's online behaviours. Parents must never underestimate how often children and young people come across potentially harmful and inappropriate material on the internet, and may be unsure about how to respond. We raise awareness about internet safety through letters home, information on our website and parent workshops. This policy is also shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised with the Headteacher or a DSL.

Acceptable use of the internet in school

All pupils, parents, staff and governors are expected to sign an agreement (via Microsoft Forms) regarding the acceptable use of the ICT systems and internet. Use of the internet must be for education purposes only, or for the purpose of fulfilling the duties of an individual's role.

Staff and Governors acceptable use agreement can be found in appendix A.

Cyber-bullying

Cyber-bullying take place on online, such as through social networking sites, messaging apps or through gaming devices. Like other forms of bullying, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

We actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying such as during PSHE lessons.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see the Child Protection policy for more information).

If there was an incident of cyber-bullying, we will follow the processes set out in our Behaviour and Discipline policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material.

If necessary, the DSL will examine the electronic device under the power of the Education and Inspections Act 2011. When deciding whether there is 'good reason' to examine the electronic device, the DSL must reasonable suspect that the data or file in question has been, or could be used to: cause harm, disrupt teaching or break any of the school rules. If there is inappropriate material, then the DSL will retain the device for evidence and will report immediately to the police.

Mobile phones

Beginning September 2026, Brushwood will become a smartphone free school. This means smart phones will not be allowed on the school site. This has been communicated with parents in advance and alternative, such as brick phones, have been suggested should their child require a phone for walking to and from school independently.

Smart watches

Children should not be bringing smart watches into school due to safeguarding issues that could arise from this. Parents should be contacted if smart watches are seen within school and they should be given to the office for safe keeping.

Youth produced sexual imagery known as Sexting

We recognised youth produced sexual imagery (known as 'sexting') as a safeguarding issue; therefore all concerns will be reported to and dealt with by the DSL. The school will follow the advice as set out in the non-statutory UKCCIS guidance: '[Sexting in schools and colleges: responding to incidents and safeguarding young people](#)'. We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability-appropriate educational methods.

All incidents of sexting will be reported directly to a DSL and they will follow the procedures set out in our Child Protection policy.

Online Hate, Radicalisation and Extremism

Online hate content, directed towards or posted by specific members of the community, will not be tolerated and will be responded to in-line with existing school policies, including anti-bullying and behaviour and discipline policy. The police will be contacted if a criminal offence is suspected.

Brushwood will take reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet in school. If the school is concerned that a pupil or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in-line with Child Protection Policy.

Reporting issues of misuse

If a pupil misuses the ICT systems or internet, then we will follow procedures set out in the Behaviour Discipline Policy, Anti-bullying Policy and internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

If a staff member misuses the ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary policy and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, if we consider whether incidents involve illegal activity or content, or otherwise serious incidents, these will be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and risks of online radicalisation. Additional training on awareness of cyber security and maintaining cyber security practices will also be delivered. All staff members receive online safety refresher training annually, as well as relevant updates as required through emails, staff meetings or briefings.

Staff training consists of:

- Updates on technology and how it can be a significant component in many safeguarding and wellbeing issues as pupils are at risk of online abuse.

This will support staff by:

- Developing better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short-term

Pupils can abuse their peers online through:

- Abusive and harassing messages
- Non-consensual sharing of indecent nude and semi-nude images/videos especially in group chats
- Sharing abusive images and pornography to those who don't want to receive such content

Physical abuse, sexual harassment and sexual violence can all contain an online element.

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety, at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

More information about safeguarding training is set out in our Child Protection policy.

Monitoring

DSLs monitor all behaviour and safeguarding issues related to online weekly using CPOMS.

This policy is reviewed bi-annually and will be shared with the Governing Body. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Acceptable use for Staff and Governors

Acceptable use of the ICT systems and internet: Agreement for staff and Governors

Name: _____

When using ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with the Headteacher or SLT first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will:

I will only use the ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

- I agree that the school will monitor the websites I visit and my use of the ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the data protection policy.
- I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed: _____

Date: _____

Acceptable use for pupils

Acceptable use of the ICT systems and internet: Agreement for pupils

Name: _____

I will read and follow the rules in the acceptable use agreement policy.

When I use the ICT systems (like computers) and get onto the internet in school I will:

- Always use the ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I have permission from the Headteacher to bring a mobile phone:

- It will be turned off, named and locked away in a locker in the school office.
- I will not use it during lessons, clubs or other activities organised by the school.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil): _____

Date: _____

Parent/Carers agreement:

I agree that my child can use the ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set above for pupils using the ICT systems and internet, and for using mobile phones in school, and will make sure my child understand these

Signed (parent): _____

Date: _____