Journeying together with God

Bramley St Peter's C of E (VA) Primary School

ONLINE SAFETY POLICY

Ratified by the Governing Board on 18th September 2025
To be reviewed annually.
Review due September 2026

Bramley St Peter's C of E (VA) Primary School Online Safety policy

The Online Safety policy is referenced within other school policies (e.g. Safeguarding, Child Protection, RSHE and Anti-Bullying).

The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

Our Online Safety policy has been written by the school, building on the Leeds City Council guidance* and Government guidance. There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety policy will be disseminated to all members of staff and pupils.

The school has an Online Safety Coordinator who has up to date training with CEOP (Child exploitation and online protection) who works alongside the Designated Child Protection Officers as the roles overlap.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Bramley St Peter's C of E (VA) Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to the responsible use of the internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Education and curriculum

The internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. Use of email, mobile phones, internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.

Why internet use is important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school's internet access will be designed specifically for pupil use and will include filtering appropriate to the age of pupils. Using the 'Talk Straight' system, the school has the ability to allow/block websites deemed appropriate/inappropriate. Pupils will be taught what internet use is and is not acceptable and will be given clear objectives for its use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content
The school will ensure that the use of internet materials by staff and pupils complies with copyright law. Pupils should be taught to be aware of the materials they read and that the internet is not always checked for accuracy.

4Cs
Staff should be aware themselves and should make pupils aware, in an age appropriate manner, of the risks that using the internet and/or technology can pose. When teaching children about using the internet they should be aware of the 4Cs, as documented page 38 (para 135) of 'Keeping Children Safe in Education' (2025). These are:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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. If pupils, students or staff are deemed to be at risk, it should be reported it to the Anti-Phishing Working Group (https://apwg.org/).

Managing Internet Access
All users must agree to the 'Acceptable Use Policy' before access to the internet and email is permitted in the school.

Information system security
The capacity and security of school ICT systems will be reviewed regularly. Virus protection will be updated regularly. Staff are asked to sign to show their agreement to the acceptable use policy committing them to maintaining the security of their personal computers and the information stored within it.

Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Online Safety coordinator and a note of the offending website address (URL) taken so that it can be blocked. Internet and email use will be monitored regularly in accordance with the Data Protection Act (2018). Children must be supervised at all times when using the internet and email.

E-mail
The use of e-mail is taught throughout Key Stage 2, and therefore pupils are provided with a 'Bramley St Peter's' e-mail address (@bsp.leeds.sch.uk).

Pupils may only use the approved e-mail accounts on the school system which are provided by Schools Broadband, and are monitored by the Talk Straight system and the school. However, pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils will be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Passwords
This school makes it clear that staff and pupils must always keep their passwords private and must not share with others. If a password is compromised the school should be notified immediately. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. Please see the data protection policy for more guidance around this aspect.

Published content and the school website
The school's website will be subject to frequent checks to ensure that no material has been inadvertently posted which might put children or staff at risk. Copyright and intellectual property rights must be respected.
The Headteacher, supported by class teachers, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The school website complies with statutory DFE requirements. Photographs published on the web do not have full names attached. Pupil's photographs can only be published with the permission of the parents/carers.

Filtering and monitoring
As stated in 'Keeping Children Safe in Education', schools and colleges in England are obliged to

- Be doing all that they reasonably can to limit children's exposure to the above risks (4Cs) from the school's or college's IT system. (para 140)
- Ensure their school has appropriate filters and appropriate monitoring systems in place and regularly review their effectiveness. (para 140)
- Be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding. (para 133)

As Ofsted noted, children should be given the opportunity to learn how to assess and manage risk for themselves through carefully managed systems, rather than systems that are totally 'locked down'.

The Department for Education's filtering and monitoring standards set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs. (para 142)

The school uses the Talk Straight system to monitor usage of the internet and block/filter access to websites as appropriate. The system has a predetermined level of filtering set up for use but this can be personalised by the school. Illegal content is blocked but other websites or individual words/phrases can be added, when they are deemed inappropriate, so that they are blocked. If staff or pupils discover an unsuitable site that has not been filtered, then this site must be reported to the Online Safety Lead or Headteacher immediately who will ensure it is entered on the restricted sites list.

Key staff within school, including the Designated Safeguarding Lead, receive daily preconfigured reports and real time alerts as appropriate. These can be scrutinised and incidents followed up where necessary.

For this reason all staff and KS2 pupils will access the school computers via a personalised log in.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. A filtering system is a tool used to support and inform the broader safeguarding provision in school.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed. Mobile phones are not suitable for children in school and so must be switched off and stored in a secure location (e.g. school office). Children are only permitted to have a mobile phone in school if it is felt their age is appropriate (Y5 and 6) and a parent/carer has signed the permission letter. The sending of abusive or inappropriate text messages is not tolerated and will be dealt with by the Pastoral and Safeguarding Lead or Senior Leaders.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

Supporting parents/carers
We recognise that access to the internet is straightforward and the vast majority of our pupils will access it at home, including some of our youngest pupils in Nursery. We aim to support parents/carers and share guidance on how they can supervise their children and manage their internet use effectively. (see communication section below).

Procedures for use of cameras, video equipment and webcams

Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.

Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be password protected and accessible only to authorised members of staff. Any photographs or video footage stored must be deleted immediately once no longer needed.

Mobile Devices (Mobile phones, tablets and other mobile devices)
Mobile devices brought into school are entirely at the staff member's, pupils', parents/carers' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

Only the designated school cameras are to be used to take any photos within the setting or on outings unless the Headteacher has given permission for the use of a staff member's camera with a school memory card inserted. This memory card MUST not be taken home and therefore should be removed once back in school.

Any adult using a camera or video recorder during a trip or visit must transfer and save images and video footage into a 'password protected' folder on an establishment/service computer immediately upon their return and the images deleted from the device.

Webcams must not be used for personal communication and should only be used with an adult present. Children, young adults and staff must conduct themselves in a polite and respectful manner when representing the establishment/service in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Policy decisions

Authorising internet access

The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents/carers will be asked to sign and return a consent form.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. 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 Leeds City Council can accept liability for the material accessed, or any consequences of internet access.
The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Expected conduct and incident management

Expected conduct

The school is responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy and should understand the importance of adopting good online safety practice when using digital technologies in and out of school.

Staff and volunteers know to be vigilant in the supervision of children and use strategies and precautions when more open internet searching is required.

Parents/carers should provide consent for pupils to use the internet, as well as other technologies. They should know and understand what the school's 'rules of acceptable use for the whole school community' are and what sanctions result from misuse.

Incident management

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Any complaints about the Headteacher should be raised with the Co-Chairs of Governors. The school has strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions. All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes. Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible and the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly concerning or breaks the law.

Incidents involving pupils misusing technology outside of school, especially the use of social media, may need to have school involvement to be dealt with appropriately. These incidents will be investigated by senior leaders and/or the safeguarding team in line with other policies such as Child Protection and behaviour.

Communication

Introducing the Online Safety policy to pupils

Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored.

Staff and the Online Safety policy
The Online Safety and Acceptable Use policies are made available within the staffroom. The policy is to be part of the school induction pack for new staff. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Enlisting the support of parents and carers
Parents/carers' attention will be drawn to the school online safety rules in newsletters, and on the school website. They will be reminded about the importance of children remaining safe online, both in and out of school. Information will be shared about how children are kept safe online within school including details of monitoring and filtering, the sites they are likely to access as part of the curriculum and who they could interact with online. Advice will also be offered to parents/carers so they know how to help keep their child safe online at home. These include monthly online safety newsletters and annual guidance on parental controls, posted on Seesaw and the school website.

Community use of the Internet
The school will liaise with local organisations to establish a common approach to online safety.

* The Governing Board have adopted the 'LCC Guidance for Staff working in Educational Settings on the Use of Digital Technologies and Social Media'.

Written by R Cartwright – Computing and e-safety coordinator (March 2015)
Reviewed by H Carter (SLT), R Richards (SLT) and C Cave (online safety and computing coordinator) - (May 2016)
Reviewed by C Cave (computing coordinator) – June 2017
Reviewed by C Cave (computing coordinator) and R Esplin (Headteacher and Designated Safeguarding Lead) – June/Sept 2018
Reviewed by R Esplin (Headteacher and Designated Safeguarding Lead) – Sept 2019
Reviewed by C Cave (computing coordinator) and R Esplin (Headteacher and Designated Safeguarding Lead) – Sept 2020
Reviewed by R Esplin (Headteacher and Designated Safeguarding Lead) and C Cave (computing coordinator) – Sept 21
Reviewed by R Esplin (Headteacher and Designated Safeguarding Lead), L Newlands (Online Safety Lead) and C Cave (computing curriculum leader) – Sept 22
Reviewed by Ruth Esplin (Headteacher and Designated Safeguarding Lead) and CP team – Sept 2023
Reviewed by Ruth Esplin (Headteacher and Designated Safeguarding Lead), SBM and CP team – Sept 2024
Reviewed by Ruth Esplin (Headteacher and Designated Safeguarding Lead), SBM and CP team – Sept 2025