Online Safety Policy

Date: Autumn 2026

Brierley Primary School



Little Bears @ Brierley

Introduction

Information and Communication Technology (ICT) is an essential resource to support learning and teaching as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to use these technologies in order to arm our children with the skills to access life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within society as a whole. The internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Artificial Intelligence (AI)

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently or effectively policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Brierley, we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, iPad, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc.).

1. Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named computing subject leader in our school is Paul Taziker. All members of the school community have been made aware of who holds this post. It is the role of the computing subject leader and designated safeguarding lead (Hayley Cunningham) to keep abreast of current issues and guidance through organisations such Cheshire East LA, Naace, CEOP (Child Exploitation and Online Protection) Keeping Children Safe in Education 2026 and Childnet.

The Head/Computing Subject Leader updates Senior Management and Governors and all governors should have an understanding of the issues at our school in relation to local and national guidelines and advice.

Online Safety development for staff

- Our staff receive regular information and training on online safety issues through the coordinators at staff meetings and briefings.
- Staff have annual online safety training.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction. Existing staff sign the form on a yearly basis (September).
- All staff incorporate online safety activities and awareness within their lessons.

Online safety information for parents/carers

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website will contain useful information and links to sites like Thinkuknow, Saferinternet, Childline, CEOP and the CBBC Web Stay safe page.
- The school will send out relevant online safety information throughout the year via email, the school website and the school prospectus.

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the online safety policy.

2. Teaching and Learning

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Our school is a mobile phone-free environment. We follow the statutory guidance on mobile phones in schools and have a policy whereby pupils do not have access to their mobile phone throughout the school day including during lessons, the time between lessons, breaktimes and lunchtime. We do this by collecting in phones as the children enter the school premises and keeping them locked away in the school office. Phones are then returned at the end of the school day. Only year 6 pupils are authorised to bring their mobile phones into school for safety if they have permission from parents to walk to and from school unaccompanied by an adult.

The breadth of issues classified within online safety is considerable and ever evolving but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer at risk, 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, including those generated using AI and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done formally and informally when opportunities arise and as part of the computing curriculum and through termly online safety themed assemblies.

- Pupils are made aware of the impact of online bullying (cyber bullying) and how to seek help if these issues affect them. Pupils are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be taught how to evaluate Internet content

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with outside providers.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail 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.

Published content and the school web site

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.

Publishing pupils' images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs i.e. of school assemblies, performances etc. for their own personal use, the school will remind parents that due to photo permissions this would not be allowed. Approved photos will be taken by the school and shared with parents via website, School Spider or Brierley Facebook page where appropriate.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils and will be strongly discouraged. However, we accept that some pupils will still use them. They will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites and to consider whether their "digital footprint" is appropriate.
- As part of safer recruitment practices, senior leaders advise that a social media search may be conducted on existing and potential new staff members.

Managing filtering

- The school will work with the LA, government agencies and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, Computing Subject Leaders, Assistant Headteachers or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept till the end of the day.
- If children are found to have sent abusive or inappropriate text messages to other pupils, we will work with parents and carers and other agencies including, where necessary, the PCSOs and the Police.
- Staff will use a school phone where contact with parent / carers is required. Should staff use their own personal phone to contact a parent i.e on a school trip, they will ensure to withhold their number.
- Staff should not use personal mobile phones during designated teaching sessions (see Personal Telephone Policy)

Cyber Bullying

We recognise that some children might be reluctant to report a cyber-bullying incident to a teacher but might disclose an incident to a parent. Therefore parental co-operative is essential, we encourage parents to report incidents and welcome their approaches for advice. Parents of the aggressor will always be informed when an incident of cyber-bullying occurs.

As referenced in Keeping Children Safe in Education 2026, we recognise that Cyber-bullying is a form of child-on-child abuse. All staff understand, that even if there are no reports of child-on-child abuse in school, it does not mean it is not happening, it may be the case that it is just not being reported. It important if staff have any concerns regarding child-on-child abuse they should speak to their designated safeguarding lead (or deputy). It is essential that all staff understand the importance of challenging inappropriate behaviours between peers, that are abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh",

"part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

Protecting personal data
The school will collect personal information about pupils and staff. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or carers if it is necessary, to pass information beyond the school or LA. For other members of the community the school will inform them in advance if it is necessary to pass the information on to anyone else other than the school and LA.

The school will hold personal information on its systems for as long as people remain a member of the school community and remove it in the event of their leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Cheshire East and as defined by the Data Protection Act 1998.

4. Policy Decisions

Authorising Internet access
- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must abide by the school's Online Safety rules. Online Safety and staying safe online is taught as part of every weekly computing lesson from years 1-6.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security
- Adult users are provided with an individual network, email login, username and password, which they are encouraged to change periodically.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

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. Brierley cannot accept full 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.

Handling online safety complaints
- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the Computing Subject Leader.
- Deliberate access to inappropriate materials by any user may lead to disciplinary procedures.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

If staff have any online safety incidents within school, they must be logged on CPOMS and a member of the senior leadership team to be alerted to it.

5. Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be discussed with the pupils regularly throughout the year. Online safety is taught and reviewed weekly within the computing curriculum for years 1-6. Additionally, it is covered in the 'Managing Self' units of the PHSE curriculum.
- Regular assemblies that discuss online safety.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the online safety policy

- All staff will be given the School Online Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

6. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Computing and Safeguarding Subject Leaders

Review: Autumn 2027

DfE REFERENCES

This Online Safety Policy is written in accordance with and guided by the following Department for Education (DfE) statutory guidance and legislation:

- Keeping Children Safe in Education (DfE, 2026)
- Working Together to Safeguard Children (DfE, 2026)
- Teaching Online Safety in Schools (DfE, 2023)
- Education Act 2002, Section 175
- Equality Act 2010
- Data Protection Act 2018 and UK GDPR

EQUALITY AND INCLUSION

Brierley Primary School recognises its duties under the Equality Act 2010 to ensure that all safeguarding and child protection practices are applied fairly, consistently, and without discrimination. The school promotes equality of opportunity and inclusion for all pupils, staff, and families. We are committed to fostering an environment where every individual is respected and supported, regardless of age, disability, gender, race, religion, sexual orientation, or any other protected characteristic.

DATA PROTECTION

All information related to online safety is handled in line with the school's Data Protection Policy, the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018. Records are stored securely and shared only when it is lawful, necessary, and proportionate to protect a child or comply with statutory requirements. Staff receive training on data protection and confidentiality as part of their safeguarding responsibilities.

GOVERNOR REVIEW AND MONITORING

The Governing Board holds overall responsibility for ensuring that this policy is implemented effectively. The Computing Subject Leader provides regular reports to governors regarding online safety issues, training, and case trends. This policy will be reviewed annually, or sooner if there are

changes to statutory guidance, and approved by the FULL GOVERNING BOARD.