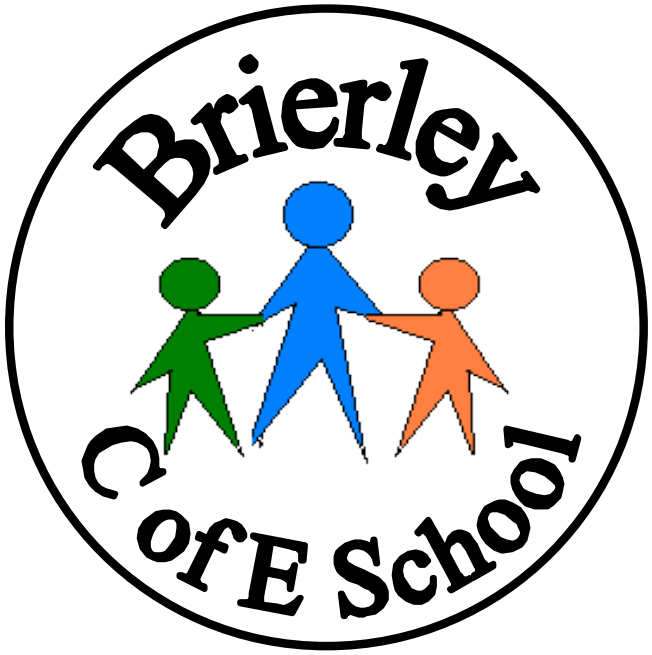

E-SAFETY POLICY

Brierley CE (VC) Primary School

E-safety policy

The e-Safety Policy relates to other policies including those for Computing, Bullying and for Child Protection.

- The e-Safety Leader is the headteacher
- The e-Safety Policy for Brierley CE (VC) Primary School has built on best practice and government guidance. It has been agreed by staff and approved by governors.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

The following sections outline the roles and responsibilities, policy statements and education in relation to e-safety for individuals and groups within the school.

Roles and Responsibilities

These are clearly detailed in **Appendix 1** for all members of the school community.

The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.

Teaching and learning

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 Internet access is provided by Barnsley Metropolitan Borough Council and includes filtering appropriate to the age of pupils. An additional filtering set is available in school administration networks only and enables staff access to additional resources.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet 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 learn that it is not appropriate to share personal information about themselves online
- Pupils will learn that inappropriate images must be reported and they will learn how to report such images.

Pupils will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by 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.

Managing Internet Access

Information system security

- School IT systems capacity and security will be reviewed regularly and monitored constantly
- Virus protection and encryption systems are installed and updated regularly.
- Security strategies will be discussed with Code Green, out IT service provider

E-mail

- Pupils and staff 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.
- If required, staff to pupil e-mail communication must only take place via a school e-mail address and will be monitored.
- 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.

All of the above are within the remit of the GDPR and additional policies to support data protection are in place

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or learning platform including in blogs, particularly in association with photographs.
- Written permission from parents / carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing on the school learning platform

- Barnsley Metropolitan Borough Council will normally block/filter access to social networking sites unless short-term access is required for a specific educational project.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school website.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The school will work in partnership with Barnsley Metropolitan Borough Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported ICT Services Help Desk.

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.
- Mobile phones will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use the school phone where contact with parents/carers or pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations. A copy of all our policies and protocols is on the school website.

Policy decisions

Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' (**Appendix 2**) before using any school IT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupils must use a class log on when accessing the internet

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither Brierley CE (VC) Primary School nor Barnsley Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher.
- Any complaint about staff misuse must be referred to the Head Teacher.
- 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 complaints procedure.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Enlisting parents' support

- Parents' / carer's attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- Parents / carers may from time to time be provided with additional information on e-safety.

The following table shows how the school currently considers these should be used.

	Staff & other adults				Students / Pupils			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff**	**Not allowed**
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices		✓						✓
Use of hand held devices e.g. i-Pads			✓			✓		
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails	✓							✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites				✓				✓
Use of blogs				✓				✓

Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate and that users should not engage in these activities in school or outside school when using school equipment or systems.		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
User Actions						
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BMBC and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping / commerce				✓		
File sharing				✓		
Use of social networking sites e.g. Facebook for older users					✓	
Use of video broadcasting e.g. Youtube				✓		

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy and acceptable use policies • Governors work with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	• Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. • Ensure that there is a system in place for monitoring e-safety • Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff • Inform the local authority about any serious e-safety issues including filtering • Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	• Lead the e-safety working group and dealing with day to day e-safety issues • Lead role in establishing / reviewing e-safety policies / documents, • Ensure all staff are aware of the procedures outlined in policies • Provide and/or brokering training and advice for staff, • Attend updates and liaising with the LA e-safety staff and technical staff, • Deal with and log e-safety incidents including changes to filtering, • Meet with E-Safety Governor to regularly to discuss incidents and review the log • Report regularly to Senior Leadership Team
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the **Staff Acceptable Use Agreement** (AUP) • Act in accordance with the AUP and e-safety policy • Report any suspected misuse or problem to the E-Safety Co-ordinator • Monitor ICT activity in lessons, extra-curricular and extended school activities
Students / pupils	• Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse • Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Ensure that their child / children follow acceptable use rules at home • Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school Acceptable Use Policy. • Keep up to date with issues through school updates and attendance at events

Appendix 1: Roles and Responsibilities (Continued)

Role	Responsibility
Technical Support Provider and data protection officer	• Ensure the school's IT infrastructure is secure in and is not open to misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data • Inform the head teacher of issues relating to the filtering applied by the Grid • Keep up to date with e-safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. • Ensure monitoring software / systems are implemented and updated • Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	• Sign and follow the AUP before being provided with access to school systems.

Appendix 2

Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, i-Pads, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will follow the GDPR as laid down in law.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for IT.

Signed: …… Capitals: …… Date: ……..……

Accepted for school: …….. Capitals: …….

E-safety Checklist

Self-evaluation		
• E-safety is referred to in the school SEF under 'that children are safe and feel safe' and 'the effectiveness of safeguarding procedures'	Yes	No
Infrastructure and Technology		
• Filtering and virus checking is in place and up to date (to GDPR standards)	Yes	No
• There is regular monitoring of web statistics to check for any issues	Yes	No
Education and Training		
• Class rules are in place and displayed in classrooms	Yes	No
• There is a teaching programme in place to ensure that all classes receive relevant education on e-safety issues	Yes	No
• Learners know how to report any concerns	Yes	No
• **All** staff have attended briefings on issues, risks and their role in relation to e-safety, non-teaching staff and relevant leaders.	Yes	No
• Member/s of staff responsible for e-safety have received relevant training to support their role	Yes	No
• **All** staff know what to do if an e-safety concern, including cyber bullying, comes to their attention.	Yes	No
Policies and Practices		
• The headteacher is responsible for e-safety issues	Yes	No
• All staff are aware of their roles in relation to e-safety and how to conduct themselves professionally on line	Yes	No
• There is an acceptable use agreement in place for pupils and pupils know how to behave on line.	Yes	No
• There is an acceptable use agreement in place for staff	Yes	No
• There is a home school agreement in place with parents	Yes	No
• An e-safety policy is in place which identifies key roles and responsibilities	Yes	No
• There are planned actions in place to improve e-safety	Yes	No
• There are systems in place to monitor the effectiveness of the teaching programme, policy and agreements.	Yes	No

BRIERLEY CE (VC) PRIMARY SCHOOL

Acceptable User Policy for Children

1. If I'm unsure about anything on the screen. I will ask the teacher or assistant.

2. I will ask an adult if I am about to use the computer or internet.

3. I will only touch my own computer or work

4. I will only put general items on the computer, no personal details.

5. I will not use chat rooms.

6. I will only use websites that I have been advised to use.

7. If any pictures or words come on to the screen that make me feel uncomfortable, I will turn off the screen and then tell a teacher.

8. I will not make any unkind comments about other people

I have read and agree to the above

Signed …….

Print Name ……..

Date …….

BRIERLEY CE (VC) PRIMARY SCHOOL

Acceptable Use Policy for Internet, Learning Environment and E-mail

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.

1 Pupils must obtain the **permission of parent(s)/carer(s)** before they can be allowed to use the Internet including educational use and e-mail service.

2 Pupils must only use the school computer systems for those activities and services which they have been given permission to use and under the **appropriate supervision** of a member of staff.

3 The Internet will be used within school to **support children's learning** both formally (within taught lessons) and informally (outside taught lessons). Informal use is at the discretion of a member of staff who will set guidelines and rules for its use. Pupils will be taught to be critical and discriminating in their use of Internet sites.

4 Pupils must only use the user name and password they have been given. Pupils will be taught to **respect the privacy** of files of other users. They will be taught not to enter, or attempt to enter without permission, the file areas of other pupils or staff.

5 Pupils should not download and use material or copy and paste content which is **copyright**. Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet. No **material from home** should be used on systems in school unless the media it is on has been virus scanned.

6 The Internet access provided in Brierley CE (VC) Primary schools is filtered to stop access to unsuitable material. As no filtering system can be 100% effective, it is important that parents are aware that users of the system are required to act responsibly. **Under no circumstances should pupils attempt to search for, view, upload or download any material that is likely to be unsuitable** for children or schools. Pupils have a responsibility to inform the member of staff supervising them if they have accidentally accessed inappropriate content.

7 Pupils may have opportunities, at times, to communicate with others via e-mail e.g. pen pals at linked schools. Pupils will only use these in accordance with the school's policy and procedure. **Responsible and considerate language** will be used at all times in communicating with others. It is important pupils understand that all mail sent using this system is screened for inappropriate language and any mail found to contain such language will be re-routed to the E-mail Manager in the school for disciplinary action which will include informing parents.

8 Pupils will be encouraged to **maintain a balance** between the use of electronic communication and face to face communication with their peers.

9 A few social network sites are now available which are appropriate and can benefit primary aged children. Parents should be aware that inappropriate sites are blocked within school and are not suitable for this age range due to the nature of the content. Pupils will be encouraged to **discuss their use of social network sites** with their parent(s)/guardians(s)/carer(s).

10 Parents are asked to **explain the importance** to their child of these rules for the safe use of the Internet and to sign and return to the school the **Parental Permission Form**. A simplified version for discussion with your child is available to parents/carers

If you do not understand any part of this "**Acceptable Use Policy**", parents should ask a member of staff for guidance.

Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

Technologies open up new learning opportunities for everyone. They can stimulate discussion, promote creativity and effective learning, and promote more effective communications between parents / carers and the school in order to support young people with their learning.

Young people should have an entitlement to safe internet access.

This **Acceptable Use Policy** is intended to ensure:

- All young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

A copy of the **Pupil Acceptable Use Policy** is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school.

We will also ensure that when images are published the young people cannot be identified by the use of their names.

Home Use of the Internet

We hope you will reinforce the issues contained in the **Pupil Acceptable Use Policy** when your child uses the internet at home.

In order to do this we recommend that you:

- Ensure that children access the internet in a communal room and that there is appropriate supervision for the age of your child (including supervising all internet use by younger users).

- Set appropriate rules for using the IT and the internet safely at home. The school rules could provide a starting point.

- Inform the school of any concerns that the school could help to address through teaching.

- Ask your child about the sites they are visiting.

- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.

- Ensure content is appropriately filtered for younger users.

- Ensure that your child knows that any protection system does not stop all unsafe content and that they need to tell you if they access something inappropriate or get an upsetting message.

- Reassure your child that if they talk to you about a problem they are having on the internet you will not ban them from using it as this will discourage them from telling you.

- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet.

Additional Guidance on Safe Use of ICT at Home

Keeping Safe

- Discuss user names with children and talk about how to choose them carefully to protect their identity.
- Talk to young people about the information they should keep private in order to prevent them being contacted or traced including full name, address, telephone no, school, places they do regularly.
- Talk to young people about the need to limit access to their own information by using the safety and privacy features of sites to only give access to people they know and being careful who they add as friends.
- Talk to the about sharing images of themselves or others and hat todo if tetreeive inappropriate images
- Model safe behaviour in your use of IT.

Research and Fun on the internet

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only publish information they would be happy for anyone to read.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves at risk.
- Check that they are old enough for the sites they are using.

Communicating

- Discuss the need for young people to be polite to others online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
- Ensure that young people know they should not open messages if the subject field contains anything offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Recognise that there is a difference between online friends who you will never meet and real world friends. Talk to your child about their online friends.
- Remind your child that people they talk to online may not be who they seem.

Sharing

- Ensure your child knows that downloading games and music that is copyrighted without paying for it is illegal

Buying and Selling Online

- Help young people to tell the difference between web sites for information and web sites selling things.
- Discuss how to recognise commercial uses of the internet e.g. i-Tunes, mobile phone downloads, shopping.
- Remind young people that if an offer looks too good to be true it probably is and that they should not respond to unsolicited online offers.
- Remind young people that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems

- Ensure that they know that if they receive an offensive or worrying message / e-mail they should not reply but should save it and tell you.

Permission Form

If you **do not wish** your child to use the internet and email then parents/carers are requested to sign the form below.

Pupil Name (PLEASE PRINT) _____ of class _____

Name of Parent /Carer (PLEASE PRINT) _____

Signature of Parent/Guardian/Carer _____ Date _____

If you are happy for your child to access the internet/emails then you need not do anything, from a **negative** response we shall assume that you are agreeing to our policy.

June 2022