



# **E-Safety Policy & Pupil Acceptable Use Agreement**

**SCHOOL POLICY**  
**Review: Annually**  
**Next Review Date: July 2026**

<b>Role</b>	<b>Name</b>
<b>Headteacher</b>	<b>Caroline Rodgers</b>
<b>Chair of Governors</b>	<b>Linda Mosley</b>
<b>Designated Governor</b>	
<b>Designated Senior Lead</b>	<b>Caroline Rodgers – Headteacher</b>

## **Introduction**

ICT in the 21<sup>st</sup> Century is seen as 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 build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (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 our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- 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 including Nintendo DS's, iPads, Tablets and other wireless message devices

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

At Brockley Primary School we understand the responsibility to educate our pupils in E-safety issues; teaching them the appropriate behaviour 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, webcams, whiteboards, digital video equipment, Chromebook, iPads etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, Nintendo DS's and other wireless message devices etc.).

## **Roles and Responsibilities**

As E-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 E-Safety co-coordinators in our school are the Headteacher and Acting Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety coordinators to keep abreast of current issues and guidance through organisations such as Derbyshire LA, CEOP (Child Exploitation and Online Protection) and Childnet.

The E-Safety coordinators update staff and governors on all ICT issues. These groups should also have an understanding of the issues at our school in relation to local and national guidelines and advice.

### **Writing the E-Safety policy**

This policy, supported by the school's IT Security and Acceptable Use Policy for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. Our E-Safety policy has been written by the school, in conjunction with advice from Derbyshire County Council, government guidance. It has been agreed by the Staff and approved by the Governing Body

### **E-Safety skills development for staff**

- Our staff receive regular information and training on E-Safety issues through the coordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-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 IT Security and Acceptable Use Policy as part of their induction.
- All staff are encouraged to incorporate E-Safety activities and awareness within their lessons.
- All school staff will need to attend regular training, this is the responsibility of the ICT Co-ordinators

### **E-Safety information for parents/carers**

- Parents/carers are asked to read through and sign the attached Acceptable Use Agreement for pupils on behalf of their child.
- 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 or school publications e.g. Newsletter. This is done as each child joins the school and as part of the annual pupil update process, the information is retained for future reference.
- The school website contains useful information and links to sites such as Childline, CEOP (Child Exploitation and Online Protection Centre), NSPCC and Safer Internet.
- The school will send out relevant E-Safety information through newsletters and the school website.

### **Community use of the Internet**

- External organisations that may use the school's ICT facilities must adhere to the E-Safety policy.

### **Teaching and Learning**

#### **Internet use will enhance learning**

- The school will provide opportunities within a range of curriculum areas to teach E-Safety, this is adopted from the CEOP learning materials.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also 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 educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- School staff are aware of safeguarding and specific child protection policies and procedures.

#### **Pupils will be taught how to evaluate Internet content**

- 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.

#### **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 Derbyshire County Council and Mercury AVS.

#### **Email**

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

The contact details on the Website should be the school address, email and telephone number. Staff or pupils' personal information will **not** be published. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

#### **Publishing pupil's 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.
- 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 Brockley 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 for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies.

A form will be made available for parents and carers to sign at each event with regards the use of images, this will remain in school after the event to ensure all parents and carers adhere to the rules.

### **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. 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, parents or former students as 'friends' if they use these sites.

### **Managing filtering**

- The school will work with Mercury, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or a staff member discover an unsuitable site, it must be reported to the Class Teacher, E-Safety Coordinators/Headteacher.
- 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 including iPads and tablets or mobile phones into school, any children bringing such items will find that they are put into an envelope, signed and witnessed by two staff members then sealed and kept in the school office until the end of the day.
- The sending of abusive or inappropriate text/electronic messages is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions. All mobiles should be kept out of view, unless required to support a medical condition in school.

### **Managing video-conferencing**

- Videoconferencing will be appropriately supervised for all pupils.

## **Protecting personal data**

The school will collect personal information about you fairly and will let you know how the school and Derbyshire LA will use it. 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 guardians, if it is necessary, to pass information beyond the school or Derbyshire LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Derbyshire LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of you 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 Derbyshire County Council and as defined by the General Data Protection Regulations (UK GDPR) and the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

## **Policy Decisions**

### **Authorising Internet access**

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's E-Safety rules. These E-Safety rules will also be displayed clearly in school.
- Access to the Internet will be by directly supervised access to specific approved on-line materials.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's E-Safety rules and within the constraints detailed in the school's E-Safety policy.
- 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 and email login username and password, which they are encouraged to change periodically.
- All pupils are provided with a network login username and password.
- 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. Neither the school nor DCC can accept liability for the material accessed, or any consequences of Internet access. The school will audit IT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

### **Handling E-Safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the E-Safety coordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety coordinator and recorded in the E-Safety incident logbook.
- 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 complaints procedure.

### **Communications Policy**

#### **Introducing the E-Safety policy to pupils**

- E-Safety rules will be displayed in school and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored.



## PUPIL GUIDELINES FOR SAFE INTERNET/EMAIL USE

- I will only use the Internet when there is a teacher present.
- I will always ask for permission before accessing the Internet/Email.
- I will only use my own usernames and passwords to log on to the system/Email and keep them secret.
- I will not access other people's files.
- I will only email people I know or my teacher has approved and ensure that the messages that I send will be polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using the Email etc.
- I will not give personal details (like my home address, telephone or mobile number), or
- the personal details of any other person to anyone, or arrange to meet someone unless my parent/carer or teacher has given me permission.
- I will only download, use or upload material when I have been given the owner's permission.
- I will only view, download, store or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials, I will inform my class teacher straight away.
- I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
- Always quote the source of any information gained from the Internet i.e. the web address, in the documents you produce.
- Use the Internet for research and school purposes only.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I understand that if I don't follow these rules, my access to the school computer system/Internet/Email may be suspended, and my parents/carers will be informed.

**KEEP THIS COPY AT HOME**



## BROCKLEY PRIMARY SCHOOL

### Acceptable Use Agreement for Pupils September 2025

Please complete and return this form to the School Office

<b>Pupil's Name</b>		<b>Class Teacher</b>	
As a school user of the Internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.			
<b>Pupil Name (print)</b>			
<b>Pupil Signature</b>		<b>Date</b>	

<b>Parents Name</b>			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.			
<b>Parents Name (print)</b>			
<b>Parents Signature</b>		<b>Date</b>	