E-Safety Policy

Date: Summer 2015

Brierley Primary School

Little Bears @ Brierley

E-SAFETY POLICY

Nurture, Aspire, Believe, Achieve

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

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 e-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, 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 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-ordinators in our school are Emma Gadsby (Designated Child Protection), Hayley Williams (Computing lead) and Chris Parker (Governor). 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 Cheshire East LA, Naace, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/e-Safety coordinator 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.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinators at staff meetings and briefings.

- 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 Acceptable Use Agreement as part of their induction. Existing staff sign the form on a yearly basis (September).
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.
- E safety is included in safeguarding training for all staff.

E-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 new 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 e-Safety information through newsletters, the school website and the school prospectus.

Community use of the Internet

External organisations using the school's ICT facilities must adhere to the e-Safety policy.

2. Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-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 e-Safety curriculum and through annual E 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 sold at a small admin cost to the parent.

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.

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, e-Safety Coordinators, Deputy 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.
- Staff should not use personal mobile phones during designated teaching sessions (see Mobile Phone Policy).

Cyber Bullying

This century has seen a rise in cyber bullying, or bullying using mobile phones and the internet. This has been compared with traditional bullying – physical hitting, damaging belongings, verbal taunts, social exclusion, rumour spreading. (The terms online and offline bullying are also used).
Cyber bullying is now a focus of major concern as well as research. It differs from traditional bullying in a number of ways – for example it is more often anonymous; it is more of an 'out-of-school' and 24/7 phenomenon, even for young people; and there can be a much wider audience for cyber bullying. There is ongoing debate and research about whether cyber bullying is just another kind of bullying, or whether we should rather think of various kinds of 'cyber aggression'. There is also debate about whether the impact of cyber bullying is any greater than traditional bullying – but it is quite clear that both kinds can have severe negative effects on victims – and at extremes, lead to suicide. (REF:See Smith (2012) and Slonje, Smith and Frisén (2012).)

Although Cyber bullying is not a specific criminal offence in UK law, criminal internet bullying laws such as the Protection from Harassment Act 1997 and the Crime and Disorder Act 1998 may apply as cyberbullying laws in terms of harassment or threatening behaviour. Where mobile bullying is concerned, the Telecommunications Act 1984 makes it a criminal offence to make anonymous or abusive calls. In addition, if you are harassed persistently on your mobile, it may be an offence under the 1997 Harassment Act. There is some anecdotal evidence that the police are more comfortable in bringing forward this law when dealing with issues of Cyber bullying. The police have successfully used the Protection from Harassment Act to prosecute for the sending of offensive e-mails through the internet. Such messages will also constitute an offence under the Malicious Communications Act and be treated as one of the cyberbullying laws. Furthermore, the Communications Act 2003 makes it a criminal offence to send: "…by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character".

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.

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 e-Safety rules. These e-Safety rules will also be displayed clearly in the computer suite.
- 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 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 coordinator.
- 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 complaints procedure.

5. Communications Policy

Introducing the e-Safety policy to pupils

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

Staff and the e-Safety policy

- All staff will be given the School e-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 Coordinators.

Review: Summer 2016

Incident Log

Brierley Primary E-Safety Log

Details of ALL E-Safety incidents to be recorded by class teachers. This incident log will be monitored termly by the E-Safety Co-ordinators. Any incidents involving Cyberbullying should be recorded and emailed to the Safeguarding Lead and Headteacher.

Date & Time	Name of Pupil or Staff Member	Male or Female	Room and computer/ device number	Details of Incident (including evidence)	Actions and reasons