

- 1.1 At Barnton Community Nursery and Primary School we understand the importance that technology plays in the lives of our pupils. Whilst we teach and encourage our pupils to embrace new technology as it emerges, its use must be balanced by educating pupils to take a responsible approach.
- 1.2 The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
- 1.3 This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
- 1.4 The nominated e-safety officer in school is Mrs. Lawson, who is the first point of contact for any e-safety related incidents.

2. Teaching and learning

- 2.1 Within the Computing section of The National Curriculum 2014, are specific, statutory objectives for e-safety for both KS1 and KS2 which staff will plan, teach and assess.
- 2.2 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.
- 2.3 Internet use will enhance learning. 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, 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
- 2.4 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.

3. Managing Internet Access

- 3.1 School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be in accordance with BECTA and Cheshire West and

Chester (CWAC) recommendations. All filtering is managed by CWAC using Smoothwall filtering system. This blocks sites that fall into categories such as pornography, race hatred, gaming and sites of an illegal nature. The LA approved system for secured emails uses encrypted devices or secure remote access where staff need to access personal level data off-site.

- 3.2 Pupils may only use approved email accounts on the school system. Pupils must immediately tell a teacher if they receive an offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Emails 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.
- 3.3 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.
- 3.4 Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified without prior parental consent. Pupils' full names will not be used anywhere in the public domain on the Web site or Blog, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupil's work can only be published with the permission of the pupil and parents. Following the same criteria, images may be published on the school Twitter feed and Facebook pages.
- 3.5 The school has filtered access to social networking sites via CWAC filter. Facebook and Twitter has been unblocked to allow access for the Headteacher to add school content to those social network sites. 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 and parents will be advised that the use of social network spaces outside school is inappropriate for pupils of primary age.
- 3.6 The school will work with CWAC (Internet Service Provider) and JTRS to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. The computing lead will liaise with the eCadets and conduct workshop based on keeping safe online with children and parents.
- 3.7 IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the internet. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the pupils' age.
- 3.8 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile Phone and devices will be switched off or switched to 'silent' mode, and staff are strongly advised to have a screen lock on their personal phone.

Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. It is expected that phones remain with personal belongings and are kept safe. Should a member of staff realise that their phone may potentially have been lost or taken then they should immediately inform the office, who should record the exact time and date and notify the Headteacher.

- The sending of abusive or inappropriate text messages is forbidden as is any other form of cyber bullying.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- If mobile phones are used for photographs and twitter, the photographs must be deleted the same day.
- If a member of staff breaches the school policy then disciplinary action may be taken.

3.9 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

4.1 All staff must read the ‘Acceptable ICT Use Agreement’ before using any school ICT resource. The school will keep a digital 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 online materials. Parents will be asked to sign and return a consent form agreeing to acceptable use policy guidelines on admission to school.

4.2 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 CWAC can accept liability for the material accessed, or any consequences of internet access. The school will audit ICT provision using Securus, to raise awareness of any concerns related to inappropriate internet use and to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 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. 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. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

- 4.4 Should any issues regarding e-safety come to light, parents and pupils should email head@barnton.cheshire.sch.uk
- 4.5 A red, 'eSafety Incident Record' should be completed by a responsible adult at the earliest opportunity. This will be passed to the e-safety nominated officer, who will investigate.
- 4.5 The school will liaise with local organisations to establish a common approach to e-safety.
- 4.6 Our eCadet team have taken responsibility for enhancing eSafety throughout school and have pledged to raise awareness of safety issues with all school stakeholders.

5. Communications Policy

- 5.1 E-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.
- 5.2 All staff will be given the school e-Safety Policy and its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- 5.3 Parents' attention will be drawn to the School e-Safety Policy in the school bulletin and on the school website.

6. Review

- 6.1 This policy reflects the consensus of opinion of the whole staff and governors and its implementation is the responsibility of all staff and governors. This policy should be considered alongside all other policies in school and will be evaluated in accordance with the policy review cycle

Julie Brandreth

Approved by: _____

Chair of Governors



Headteacher

Date: _____

September 2020

September 2020

