

Broadbent Fold Primary School and Nursery



Computing & E-Safety Policy February 2023

In line with the Equalities Act (2010) we aim to ensure that any child, irrespective of protected characteristics (These are age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.) is treated fairly and with respect. The law states that the public sector equality duty includes a general duty to, "Foster good relations between people who share a protected characteristic and those who do not." This policy can be adapted to suit individual needs.

Rationale

A high-quality education in computing equips children with the skills to use computational thinking and creativity to understand and change the world. Computing has deep links with Mathematics, Science, and Design and Technology and provides insights into both natural and artificial systems. The core of computing is computer science, in which children are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming.

Building on this knowledge and understanding, children are able to use information technology to create programs, systems and a range of content. Computing also ensures that children become digitally literate and are able to use, and express themselves and develop their ideas through Information and Communication Technology at a level suitable for the future workplace and as active participants in a digital world.

Writing and reviewing the Computing & E-Safety policy

This policy (for staff, governors, visitors and children), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying. Our Computing & E-Safety policy has been agreed by the Senior Leadership Team and Staff. The Computing & E-Safety policy and its implementation are reviewed annually.

Aims of Computing

Ensure all children:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation.
- Can analyse problems in computational terms and have repeated practical experience writing computer programs in order to solve such problems.
- Can evaluate and apply information technology including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Aims of E-Safety

Ensure all children:

- Use the internet as part of their learning experiences.
- Understand acceptable use of the internet.
- Can evaluate the internet content with their Digital Literacy.
- Inform an adult if they encounter a misuse of the internet.

All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and what to do in the event of misuse of technology by any member of the school community.

Current resource provision

The school has a computer suite and laptops, laptops can be used within classrooms to enhance learning. iPads are available for staff and children to use which can be moved to different areas of the school.

An ICT security, data protection and a cyberbullying policy (on the school website) are designed to allow the safe and efficient use of the Internet for both staff and children in an educational context.

Suggested long term planning Computing themes and key skills are available on the p drive alongside medium and short-term plans linked to the National Curriculum, updates and resources are shared with teaching staff.

E-safety lessons are taught to children throughout the year, as part of the computing curriculum but also as part of PSHE. In Computing, as with all subjects, in order to develop the continuity and progression of teaching and learning, a balance between whole class, individual and group work, and direct teaching, pupil investigation and skills practice is planned throughout the school.

Health and Safety

Food and drink must not be consumed near computing equipment.

- It is the responsibility of all staff to ensure that classroom computing equipment is stored securely, cleaned regularly and that their class or themselves leave the equipment clean and tidy after use.
- Staff should ensure that the children are seated at the computers comfortably and be aware of the dangers of continuous use (e.g. eye/wrist strain etc).
- An adult should always supervise children when they are accessing information via the Internet. The service provider does filter information but staff are advised to take great care on the content accessed by children and ultimately responsible for information accessed by children.
- Regular E-Safety lessons will keep children informed of internet safety so that children can highlight and identify possible risks.

Entitlement to the Computing Curriculum

All children should have access to the use of computing technologies regardless of gender, race, cultural background or physical or sensory disability. Where use of a school computer proves difficult for a child because of a disability, the school will endeavour to provide specialist equipment and software to enable access.

Children with learning difficulties may have greater access to the whole curriculum with these technologies. Their motivation can be increased and are able to improve the accuracy and presentation of their work which in turn can raise self-esteem.

Careful consideration is considered in planning for Computing in Early Years for children to gain confidence in the use of a variety of technologies once they start attending school.

All members of staff incorporate E-Safety activities within teaching throughout the year. Educating children on the dangers of technologies that may be encountered outside school is carried out informally and when opportunities arise and as part of the Computing & E-Safety curriculum and PSHE lessons.

Children are taught what is and what is not acceptable use of the Internet and given clear objectives for Internet use which is regularly reinforced. They are taught about the impact of online bullying and how to seek help if they are affected by these issues.

Children will also need to be 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.

Children are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Network

Internet access is designed for the children to use safely and our IT Technician ensures the network is healthy through use of anti-virus software. The software blocks access to social networking sites. Staff and children are asked to report any incidents of bullying to the school.

Managing Internet Access Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated and overseen by the technician.
- System security is overseen by our technicians
- Children may only use approved e-mail accounts on the school system.
- Children 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.

Published content and the school web site

The contact details on the school website are the school address, e-mail and telephone number. Staff or children's personal information is not published.

Publishing children's images and work

All staff must be aware that:

- Written permission from parents/carers is obtained before photographs of children are published on the school Website. Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.
- Children's full names will not be used anywhere on the school website, particularly in association with photographs.

- Children's work can only be published by outside agencies with the permission of the parents/carers.

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 etc.

- Children and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged children.
- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Internet & Network Access

- Children abide by the school's Home School Agreement.
- Access to the Internet is directly supervised and to specific, approved on-line materials.
- All staff using a school laptop are aware of the schools ICT Security policy.
- Adult users are provided with an individual network username and password, email address and username and password, which they are encouraged to change periodically.
- All children from Year 1 upwards are provided with an individual username and password.
- All members of staff are aware of the dangers inherent in leaving the MIS system, for pupil-tracking and digital registers, open and of the importance of keeping passwords secret
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.
- E-Safety rules are reinforced with children when using ICT equipment for e.g. computers, laptops or iPads.
- Children are informed that network and Internet use will be monitored. Networks are taught as part of Computing & E-Safety lessons.
- The school is vigilant when conducting 'raw' image search with children e.g. Google or Lycos image search.
- All staff sign the Staff laptop/ipad agreement and a copy is kept on file.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- All members of staff are aware that internet traffic can 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 (see laptop use policy). 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.

Assessing risks

The school takes all reasonable precautions to ensure that users access only appropriate material. An ICT audit is carried out to ensure the e-Safety policy is adequate and its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse is dealt with by a senior member of staff and reported to the headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the headteacher.
- Any complaint about staff misuse is referred to the Headteacher.
- Complaints and concerns of a child protection nature are dealt with in accordance with school child protection procedures. For example evidence of: inappropriate online relationships; a child watching pornography or any '18' films on a regular basis; online/digital bullying, harassment or inappropriate image sharing etc.
- Children and parents will be informed of the complaints.

Parents and the Computing & E-Safety Policy

- When a child joins our school, all parents are asked to adhere to the School's Home School Agreement.
- Consent to images of their child being taken/used on the school website or on Seesaw (Online Learning Platform) is requested from parents/carers.
- Parents/carers are invited to familiarise themselves with the school's Computing & E-safety policy.
- Parents/carers receive information on E-Safety through the school website or emails.

The Online Learning Platform

- Information regarding the school's website and Online Learning Platform- Seesaw and how it can enhance the learning of each child is sent to parents/carers.
- All children are given a username/password/code to access secure resources and facilities on Seesaw and other online learning resources.
- Seesaw is regularly monitored for incidents of cyberbullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending of messages through Seesaw is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user from Seesaw should such behaviour be repeated.
- Class teachers monitor the use of the Seesaw. Any misuse of Seesaw is reported on the school's system notifying the safe guarding leads.

Assessment and Record Keeping

- On-going formative assessment is an integral part of good practice. Its main purpose is to enable teachers to match work to the abilities and needs of the children and ensure progression in learning.
- Computing skills capability is monitored regularly in relation to the Computing curriculum as outlined in the 'The National Curriculum' for England. Teachers assess module requirements with reference to children's knowledge, understanding and skills. Other opportunities for assessment will arise from cross-curricular work.

- Children's computing work, where possible, should be saved on the school network within relevant class folders on the p drive.
- It may not be practical to keep samples of work for children in Nursery and Reception but observations and discussions can be recorded within their books or on the Online Learning Platform.

Links to the School Development Plan

- The Computing Subject lead produces an action plan. E-Safety & PSHE is reviewed and actions are included within the School Development plan.
- An audit of resources is undertaken to ensure that hardware and software are kept as up-to-date as possible and that obsolete or broken machines are scrapped or repaired.

Staff training

Training needs will be met by:

- Staff skills and confidence in the use of information technologies is audited on a regular basis to identify any training needs.
- The Computing Subject Lead attends training which is shared with staff to support the delivery of ICT.
- Annual e-safety training is arranged and completed by all staff working with children.
- All staff are aware of professional conduct and safer working practices regarding technologies such as on the Twitter, Facebook, Blogging etc.

Review and evaluation procedures

The everyday use of Information and Communication Technology is developing rapidly, with new technology being produced all the time, therefore this policy is reviewed annually.

The Computing Subject Lead liaises with staff at staff meetings and informally to monitor the effectiveness of the policy and the Computing curriculum. E-Safety is also reviewed regularly as part of Computing and PSHE curriculum. All subject leaders ensure the use of information technologies across the curriculum is planned for and evaluated.

This policy should be read in conjunction with our GDPR and Safeguarding policies.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis. This policy is the Governors' responsibility who review its effectiveness annually. They do this during reviews conducted between the headteacher/Safeguarding Lead and Computing Lead. Ongoing incidents are reported to the governing body.

Reviewed : February 2023