

**Broadbent Fold Primary School
and Nursery**

**Computing, Online Safety Policy
(including AI)**



February 2025

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 computing education equips pupils 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 equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – 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.

It is vital that children are taught how to keep safe online and how to recognise and distinguish between correct and incorrect information. This is especially crucial with the introduction of AI that has become part of technology.

This policy (for staff, governors, visitors and children) is to protect the interests and safety of the whole school community in an increasingly digitised world, this policy outlines our approaches to computing, online safety, and artificial intelligence (AI). It is essential that we prepare our students not only to use technology effectively but also to navigate the complexities of online interactions and emerging technologies responsibly. This policy aligns with the 2014 National Curriculum for Computing and meets the expectations of Ofsted’s latest inspection framework.

Aims of Computing

Our aims are to 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 Online-Safety

Our aims are to ensure all children:

- Use the internet as part of their learning experiences.
- Know acceptable use of the internet.
- Can evaluate the internet content with their Digital Literacy.
- Inform an adult if they know of a misuse of the internet.
- Create a culture of responsible online behaviour among children, staff and the wider school community.
- Foster an understanding of the ethical implications of AI and its impact on society.
- Recognise that information online may or maybe not be correct and true.

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

Present 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 pupils in an educational context.

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

Online 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 should be 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/laptops/ipads 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 pupils.

- Regular Online Safety lessons will keep children informed of internet safety so that children can highlight and identify possible risks. PSHE lessons delivered cover Online Safety. This prepares children for the work place and for using technology effectively.

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. SEND children may use technology such as a laptop or ipad to support them in accessing the curriculum, acting as assistive technology.

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.

Planning for Computing in the early years has to be considered carefully if children are to begin to gain confidence in the use of a variety of technologies as soon as they start attending school.

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

Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, this needs to be regularly reinforced. Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Through regular teaching of Online & PSHE children will be aware of the impact of online bullying and know how to seek help if these issues affect them. 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.

Network

The school Internet access will be designed expressly for children to use and will include filtering appropriate to the age of children. Technician ensures network healthy through use of an anti-virus software. The school 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 or carers will be obtained before photographs of children are published on the school Website. 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.
- 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 pupils.
- 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 will be by directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made 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 Y1 upwards are provided with an individual username and password.
- All members of staff are aware of the dangers inherent in leaving the SIMs 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.
 - Online rules are reinforced with children when using ICT equipment for eg. computers, laptops or ipads. This needs to be reinforced regularly.
- Children will be informed that network and Internet use will be monitored. Networks are taught as part of Computing & Online lessons.
- The school is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search
- All staff must sign the Staff laptop/ipad forms 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 will take all reasonable precautions to ensure that users access only appropriate material. The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be 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 must be referred to the Headteacher.
- Complaints and concerns of a child protection nature must be 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 & Online Safety policy

- 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 on Seesaw (Online Learning Platform)
- Parents are encouraged to look at the school's Computing & Online safety policy.
- Parents receive information on Online Safety through the school website or emails.

The Online Learning Platform

- Parents will be informed about the school's website and Online Learning Platform- Seesaw and how it can enhance the learning of each child.
- All children will be given a username/password/code to access secure resources and facilities on Seesaw and other online learning resources.
- Seesaw will be 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 will monitor the use of the Seesaw. Any misuse of Seesaw will be reported on the school's system so that the safe guarding leads are aware. Other online platforms such as Mathletics will also have individual passwords.

Assessment and Record Keeping

- On-going formative assessment is an integral part of good practice. Its main purpose is to enable the teacher 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 leader produces an action plan. Online & 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

Needs will be met by:

- Auditing staff skills and confidence in the use of information technologies regularly, arranging training for individuals as required.
- The Computing Subject Leader supports staff in delivering Computing, attends training which is shared with relevant staff.
- Annual e-safety training is arranged and completed by all staff working with children.
- All staff must be 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. This policy therefore will be reviewed and revised on a yearly basis. The Computing Subject Leader will liaise regularly with staff, both at staff meetings and informally, to monitor the effectiveness of the policy and the Computing curriculum. Online safety will be also be reviewed regularly as part of Computing but also as part of the PSHE curriculum. All subject leaders will also ensure that 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 and they will review its effectiveness annually. They will do this during reviews conducted between the headteacher/Safe guarding Lead and Computing Lead. Ongoing incidents will be reported to the full governing body.

Reviewed : February 2025