E-Safety Policy

Date of Policy	Review Date	Policy Written by:	Date Shared with Staff	Date Shared with Local School Board
February 2024	No later than two years following publication of the policy	Mrs Selina Ratchford (Headteacher)	February 2024	February 2024

This policy is an umbrella e-safety document and should be read in conjunction with our safeguarding and child protection policies.

In addition, we have:

- *A Home School Agreement (including a section for parents to sign and discuss with their children).*
- *Behaviour Policy*

Background and rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of this policy

This policy applies to all members of the Spalding St Paul's community (including staff, pupils, parents/carers, visitors, volunteers and community users) who have access to and are users of the school ICT systems, both in and out of school.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents and inappropriate behaviour that take place out of school.

Ethos

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. 'The Keeping Children Safe in Education' document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support e-safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

E-safety is a partnership concern and is not limited to school premises, school equipment or the school day. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This means that we will intervene in incidents that also occur outside of school if bought to our attention. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Anti-Bullying and Code of Conduct Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

Roles and Responsibilities

The Headteacher will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Member of Staff for E-Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers. The Governing Body of the school will ensure that:
- There is a senior member of the school's leadership team who is designated to take the lead on e-safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate computing and e-safety training.

The designated member of staff for E-Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on e-safety.
- Ensure that all staff and volunteers have received and signed a copy of the school's Acceptable Usage Agreement.

- Ensure that all staff and volunteers understand and aware of the school's e-safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Regularly check files on the school's network and report any concerns to the designated person.

Education: Pupils

Whilst regulation and technical solutions are very important, we recognise at Spalding St Paul's Primary School that their use must be balanced by educating pupils to take a responsible approach. Children should build their resilience to online issues through progressive and appropriate education. This is delivered through a planned and progressive e-safety programme and is an essential part of the school's computing and PHSE provision.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum.

The online safety curriculum will be provided in the following ways:

- Age appropriate e-safety is taught at the beginning of every Computing lesson.
- Age appropriate e-safety is taught through PHSE lessons.
- Lessons promote e-safety through strands of teaching pupils how to:

    - Think before you share (be internet Sharp): *Children are taught that good (and bad) news travels fast online, and children can sometimes find themselves in tricky situations with lasting consequences. Children are taught what they can do to prevent this and share smartly with those they know – and those they don't.*

    - Check it's for real (be internet Alert): *Children learn that people and situations online aren't always what they seem. Children learn how to tell the difference between what's real and what's not.*

    - Protect your stuff (be internet secure): *Children learn that personal privacy and security are as important online as they are in the real world. They explore the concept of ownership of online content and look at how to keep valuable information safe to help them avoid damaging their devices, reputations and relationships as well as addressing potential consequences of illegal access, download and distribution.*

    - When in doubt discuss (be internet Brave): *Children learn that when they come across something they're not sure about online, they should feel comfortable talking to a trusted adult. Adults can support this by showing they're open to talking, even about difficult or embarrassing things at home and in the classroom. Children also explores the impact that technology has on health, wellbeing and lifestyle e.g. mood, sleep, body health and relationships. Children also explore understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.*

    - Respect each other (be internet kind): *Children investigate how the internet amplifies everything: good things seem more exciting, bad things seem much worse and can hurt – a lot. We teacher children a great rule to live by online, as well as off, is 'treat others as you would like to be treated yourself'. Children are taught that they can have a positive impact on others and stop bullying in its tracks by refusing to join in.*

    - Respect yourself (be internet aware): *Children explore the concept of reputation and how others may use online information to make judgements. Children are offer opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles. It also helps children explores the differences between online and offline identity beginning with self-awareness, shaping online*

identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

How will internet use enhance learning?
The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for internet use. They will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

How will filtering be managed?
The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to ICT systems.
- All users will be provided with a username and password in KS2.

The school has a robust filtering system in place which is implemented and managed by Ark IT Solutions. Systems to protect pupils are regularly reviewed and improved.

How will pupils learn to evaluate internet content?
If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the appropriate support staff of Ark IT Solutions via Computing coordinator.

We will ensure that the use of the internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will need to learn how to evaluate internet information and to take care of their own safety and security.

Training should be available to staff in the evaluation of web materials and methods of developing student's critical attitudes.

Introducing the policy to pupils
Rules for Internet access will be posted in all rooms where computers are used.

Responsible internet use, covering both school and home use, will be included in the PSHE and Computing curriculum.

Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet.

Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

Education: Parents/carers

Many parents and carers understand some online safety risks/issues and they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

At Spalding St Paul's Primary School we will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities: sharing of curriculum newsletters/knowledge organisers.
- Letters, newsletters, school website and social media pages.
- Workshops for parents/carers.
- High profile events/campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publications.
- Children educating parents.

Education: The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning sessions or resources in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The schools website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools.

Education & Training: Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of online safety training will be made available to all teaching and non-teaching staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use if pre-planned, it is best practise that pupils should be guided to sites checked as suitable for their use and that processed are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites pupils visit.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.