Spring Bank Primary School Online Safety Policy 2025

Spring Bank Primary is committed to safeguarding all children and expects our staff and volunteers to share this commitment.

Approved by Governors: December 2022
Review Date: November 2025

This policy is part of our safeguarding commitment and relates to other policies including those for Computing, behaviour and anti-bullying, PHSE and child protection.

Our Online Safety policy and computing curriculum aims to empower, protect and educate pupil and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Whilst the school recognises the significant breadth of potential dangers, our Online Safety Policy has been written to reflect the four main working area outlined in Keeping Children Safe in Education 2021.

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contac**t: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If the DSL has been made aware of pupils or staff who are at risk, they will report it to the Anti-Phishing Working Group.

Why We Teach Online Safety

Why Internet use is important.

- The Internet is an essential element 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.

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 and 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.
- Pupils will adhere to the Acceptable Use Policy for all pupils in school.

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. At Spring Bank Primary we use **D-Side** specialist teachers to support this approach at the start of the autumn term.

What We Teach

Online safety is taught explicitly through a scheme of work in in all year groups through the Purple Mash 2BeSafe Online scheme. The scheme covers:

- Self-image and identity
- Online relationships and reputation
- Bullying
- Managing information
- Health wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

In Key Stage 1, pupils will be taught to:

• Use technology safely and respectfully, keeping personal information private

• Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

• Use technology safely, respectfully and responsibly

• Recognise acceptable and unacceptable behaviour

• Identify a range of ways to report concerns about content and contact

• Recognise spam and scam risks

• Understand the potential benefits and risks of AI

By the end of primary school, pupils will know:

• That people sometimes behave differently online, including by pretending to be someone they are not.

• That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

• How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

• How information and data is shared and used online

• How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Parents and Online Safety

The school raises parents' awareness of internet safety through communication on Class Dojo and information via our website Online safety will also be covered during parents' information evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head teacher.

Cyber - bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school actively discusses cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers discuss cyber-bullying with children, and the issue are addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school follows the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to

• Cause harm, and/or

• Disrupt teaching, and/or

• Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

• Delete that material, or

• Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

• Report it to the police Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly. All internet access is filtered by the school's ISP.

If staff or pupils discover an inappropriate website it must be reported to the designated safeguarding lead. We recognise that no filter can ever be perfect, therefore, children will be taught the necessary skills to manage risks themselves on an age appropriate level. Virus protection is updated and files scanned continuously. Any unsafe searches are detected by the filtering software; the DSL, Head teacher and Computing Lead receive notifications.

The Prevent Duty

The filtering systems in place are compliant with the Prevent Duty and any internet use that is in violation of this duty is automatically reported to a designated member of staff for safeguarding. All staff have up to date Prevent duty training and this will be updated as required.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Please see the current Acceptable Use Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and children will be supervised and monitored when using these.

Pupils are not permitted to have in their possession, any personal electronic device which allows internet access. Mobile phones used for the purposes of walking home must be handed in to the teacher at the beginning of each day

Managing data security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2016.

Accessing risks

The school will take all reasonable precautions to ensure that users only access 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 Schools Broadband can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

Staff using work devices outside of school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy and acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Policy Decisions

Authorising Internet access

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet may be in response to a supervised search. School filters should ensure that only suitable materials can be accessed.

- Pupils will be asked to sign an acceptable use form which will then be copied and sent home.

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. Neither the school nor Children Leeds can accept 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.

Introducing the Online Safety Policy to pupils

- **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.**

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website.
- The school will provide Online Safety Information via the school website.

Spring Bank Primary School Online Safety Policy 2025

Appendix i

Summary of Requirements of KCSIE 2022

- **The DSL has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.**
- **DSLs should evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.**
- All staff (including governors and trustees) should receive appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- **Online safety should also be addressed as part of regular (at least annual) child protection training and staff should receive updates, as appropriate.**
- **Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE),** however schools and colleges should recognise that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, may be needed.
- Schools/colleges should be doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system and should ensure they have appropriate filtering and monitoring systems in place and regularly review their effectiveness**. The leadership team and relevant staff should have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns identified. When making filtering and monitoring decisions, schools/colleges should consider those who are 'potentially at greater risk of harm' and how often they access the IT system along with the proportionality of costs versus safeguarding risks.**
- Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have appropriate systems in place to support and evidence this.

- Schools/colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to appropriate filtering and monitoring on school devices and school networks, child-on-child abuse, relationships on social media and the use of mobile and smart technology.
- **Schools/colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks their children face.**

The implications for DSLs and Leaders:

- Online safety should be viewed as part of your school/college statutory safeguarding responsibilities and will require a whole school/college approach.
- **Ensure your DSL is recognised as having overall responsibility for online safety, and that they access appropriate training and support to enable them to keep up to date.**
- **Ensure your safeguarding policies (including your child protection policy), education approaches and staff training address the breadth of online safety issues as identified in KCSIE; content, contact, conduct and commerce.**
- Update your child protection (and/or online safety policies if you have a standalone document) and behaviour policies to address appropriate filtering and monitoring on school devices and school networks, online child-on-child abuse, and the use of mobile and smart technology on your premises.
- Ensure your staff behaviour policy specifically covers acceptable use of technologies, including the use of mobile devices, staff/pupil relationships and communications, including the use of social media.
- Work with curriculum leads (especially RSE leads) to ensure there is a range of opportunities within the curriculum for children to be taught about online safety in a way that is appropriate to their age and needs.
- Ensure all staff, including governors and trustees are provided with appropriate and up-to-date online safety information and training at induction, and as part of regular child protection training and updates.
- **Staff training should include an 'understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring'.**
- All staff should be made aware of the policies and procedures to follow with regards to responding to online safety concerns, including online child-on-child abuse issues.
- DSLs should access the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and the DfE 'Harmful online challenges and online hoaxes' guidance to ensure they are familiar with its content and when it should be followed.

- Schools/colleges should ensure appropriate filtering and monitoring approaches are in place which are suitable for the local context and use of technology. The leadership team and relevant staff should have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- DSLs and school/colleges leaders should access the DfE 'Filtering and monitoring standards for schools and colleges' and 'Cyber security standards for schools and colleges' and consider how the school/college is meeting the requirements, and if any further action is required.
- The school/college recruitment process should be transparent and ensure that shortlisted candidates are aware that online searches may be done as part of due diligence checks.
- **There should be regular and appropriate parental engagement in online safety, and specific concerns should be responded to in line with child protection policies.**
- DSLs should ensure online safety approaches are regularly reviewed and supported by an annual risk assessment that considers and reflects the specific risks their children face.