Springfield Junior School

Online Safety Policy

Prepared by	*Louise Everitt/Kim Cook*
Approved by the Committee/Governing body	*April 2023*
Review date	*April 2024*

Online Safety at Springfield Junior School

At Springfield, we firmly believe that all staff members have a responsibility to provide a safe environment in which children can learn. As digital devices form a central role in all of our lives, we promote children to create positive digital footprints online and teach individuals to become independent by raising concerns they may have.

We endeavour to create an open culture within school where children are not afraid to report concerns they may have. With regular communication with parents through newsletters and using the school's website, helpful advice is regularly given to parents from the Online Safety Lead and appropriate channels are identified for parents to raise questions they may have, including practical support they can use at home through sharing of regular 'Wake up Wednesday' online safety information.

The Online Safety Policy relates to other school policies including Acceptable Use for ICT/staff, Acceptable Use for ICT/pupils, Staff Code of Conduct and the school's Safeguarding Policy. These policies should be read in conjunction with the Online Safety Policy.

Keeping Children Safe in Education

The Online Safety Policy was written, and informed, using Keeping Children Safe in Education (September 2022).

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Child-on- Child Abuse and Child Sexual Exploitation

At Springfield Juniors, stakeholders are aware that children can abuse other children (often referred to as child-on-child abuse). This can happen both inside and outside of school and online. All members of staff are aware that digital devices can sometimes lead to child-on-child abuse.

During lessons and assemblies, we promote the importance of how we positively interact in the online and offline world. Child- on child abuse includes abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Channels are provided in school where pupils can report these concerns to a trusted adult, but members of staff are aware of what indicators to look out for in class. Safeguarding is our ultimate priority at Springfield Juniors.

Staff members are aware of how electronic devices could be used to exploit children sexually. This may include non-contact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet. A culture of sharing is being created in school where pupils are comfortable to share concerns, resulting in appropriate resolutions.

Safeguarding and Online Safety Team at Springfield Junior School

Our Senior Designated Lead for Safeguarding is **Mrs L Everitt** (Headteacher). The Alternate Senior Designated Leads for Safeguarding are **Mrs K Cook** (Deputy Headteacher), Miss B Taylor (Assistant Headteachers) and Mr D Rycraft (Family Support Worker).

Our Online Safety Lead is **Mrs K Cook** (Deputy Headteacher). The Computing Governor is **Richard Smithson** and the Safeguarding Governor is **Samantha Green**.

The Aims of our Online Safety provision (Intent)

At Springfield, we believe that being online is an integral part of children and young people's lives. Our ambition is to make children aware of the many positive outcomes from being online; however, it is also important that children are aware of the risks may face.

Being a Rights and Respect School, we firmly believe that every child has a right to be safe online. Through events in school, children are empowered to voice their concerns and gain timely resolutions.

Many children are connected with each other using a range of digital devices: social media, online games, website and apps. We firmly believe that all children, regardless of age, disability, gender, race, religion or belief, or sexual orientation, should have an equal protection from all types of harm or abuse.

Within school, our aim is to teach pupils the link between their own behaviour when interacting in person, and also the behaviour they display when online. We want pupils to be aware of their actions online, including the content they post and the contact they make, and take responsibility for their actions.

Our aim is to not only support children with online safety in school, but promote pupils to identify concerns they have when using electronic devices at home.

We strive to create a culture in school where pupils can report their concerns, whatever the severity of the incident. We firmly believe that promoting a culture of openness supports children to have the confidence to report any concerns they may have online. Our intent is to not only work in collaboration with pupils, but also support parents and other stakeholders.

At Springfield, we understand, like all elements of safeguarding, the importance of all stakeholders working together to promote the positive values of being online and also the risks it can pose.

How we put our aims into daily practice (Implementation)

All stakeholders have a responsibility to uphold positive values when online. Pupils, staff and parents sign AUPs (Acceptable Use Policies) to uphold appropriate behaviour online when working in school or off-site.

During periods of remote learning, the loan of any laptop is preceded by signing an AUP for remote learning. Clear expectations for all stakeholders are outlined in all AUPs and can be found on the school's website.

Within school, pupils are taught about the importance of creating a positive digital footprint online. Online safety is no longer relegated to receiving one day inputs across the year – online safeguarding is fed into the culture at Springfield Primary School:

- The school's website offers a range of top tips for pupils on how to behave online and the homepage contains links to CEOP, allowing pupils to report any incidents.

-Weekly 'Wake up Wednesday' emails are sent to parents with a digital guide drtailing advice around online usage for children.

-Regular teaching opportunities are used in school through class learning or online safety themed assemblies.

- Children are provided the time to discuss how they interact with others online and also learn practical advice which they can apply when using electronic devices.

- External agencies, including our School Liaison Police Officers, make regular visits to school and discuss themes of online safety. Children are taught about what data should be shared about themselves; pupils are clear they should not provide details of any kind which may identify them, their friends or their location.

In school, children are also promoted to be independent and autonomous learners. Self-referral sheets are available in all classes where children are able to outline any concerns they have online. The referral sheets are then actioned by the class teacher and supported by the Online Safety Lead. These are regularly reviewed during assemblies and all concerns are recorded using our secure safeguarding platform.

Parents are sent regular emails regarding useful information about online safety. The school's newsletter is also used as a platform to disseminate information which provides practical advice on how parents can pro-actively support their child at home.

On-site, Gipping Valley and Mr. R Beech manage the school's network and software. Appropriate updates are applied to ensure that we are compliant with appropriate filtering and monitoring, up-to-date antivirus software.

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

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

We are successful because… (Impact)

The curriculum, and culture in Springfield, is designed to ensure pupils feel confident to raise concerns which relate to online safety. We work in collaboration with other agencies to support parents with issues they may face online.

-Pupils are able to report concerns in, or outside of school, including child-on-child abuse, by using self-referral forms. These can be found in all classrooms and are then provided to the Online Safety Lead, who will act upon these promptly.

-Workshops, in school or virtually, provide parents with practical tips to keep children safe online. Assemblies with online safety themes are led by the Computing Lead and relationships have been created with our School Liaison Officer, Jason Cowles.

-External agencies, including the Neighbourhood Police Team, work in collaboration with staff in school to support all parents. Children are provided with regular workshops which provide top tips to stay safe online. Online sessions are also provided to parents which outline constructive ways to keep their children safe online.

-Regular updates are provided to parents via Arbor or the school website (https://www.springfieldjuniors.org.uk/online-safety.html) which provide up-to-date information about changes to online platforms and how to safeguard pupils at home appropriately.

-The website also has an electronic form where parents can raise their own concerns and these are then sent to the Online Safety Lead. This enables all stakeholders to communicate concerns with the school effectively.

-Safer Internet Day, and other events throughout the year, are participated in which allows pupils to reflect on how they behave online and the digital footprint they create.

In School: Being Online, including GDPR

Internet Access

The school's internet access is designed expressly for pupil use and will include filtering by our service provider, currently through Suffolk County Council.

If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Lead. Appropriate steps are taken to ensure that the site is blocked and, if necessary, any relevant stakeholders are communicated to.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any member of staff finding any areas deemed

inappropriate should inform the Online Safety Lead so they can be recorded and reported to the IT Technician/internet provider for blocking. School ICT systems security will be reviewed regularly; virus protection will be updated regularly.

E-mail and Google Classroom

Pupils may only use approved, school-provided e-mail accounts on the school system. Children currently use Google Classroom to communicate with class teachers. Any emails sent by children will be contained within the Springfield domain and external parties are unable to communicate with pupils directly. Parents may use the class' email address to communicate with the class teacher during periods of remote learning.

Pupils will be enrolled to on-line sites to allow for use of software (for example Accelerated Reader in literacy), website design and other ICT skills, the ICT lead and Systems Technician will keep a full record of all sites used by the school and those children registered to individual sites.

Published content and the school website

Staff or pupil personal contact information will not be published. The contact details given are to the school via general email and telephone contact information. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

First names will only ever be published on the school website when celebrating pupils' learning. As part of Online Safety training, the school will not publish pupils' full names anywhere on a school website or other online space in association with photographs.

On admission, parents are asked to sign an agreement, part of which relates to permission for photographs to be published on the school website and supports our robust approach to GDPR.

GDPR

Springfield Junior School is the 'data controller' for the purposes of data protection law. Please refer to the school Data Protection Policy and Privacy Notices for more information.

Our data protection officer is Louise Everitt, Deputy Head. Sam Pollard, Broke Hall, takes overall responsibility for GDPR across the Children's Endeavour Trust. Further information can be found on our school website regarding GDPR and how we store information (https://www.springfieldjuniors.org.uk/data-protection-gdpr.html)

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, e-bulletins and staff meetings). These are usually through the National College.

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

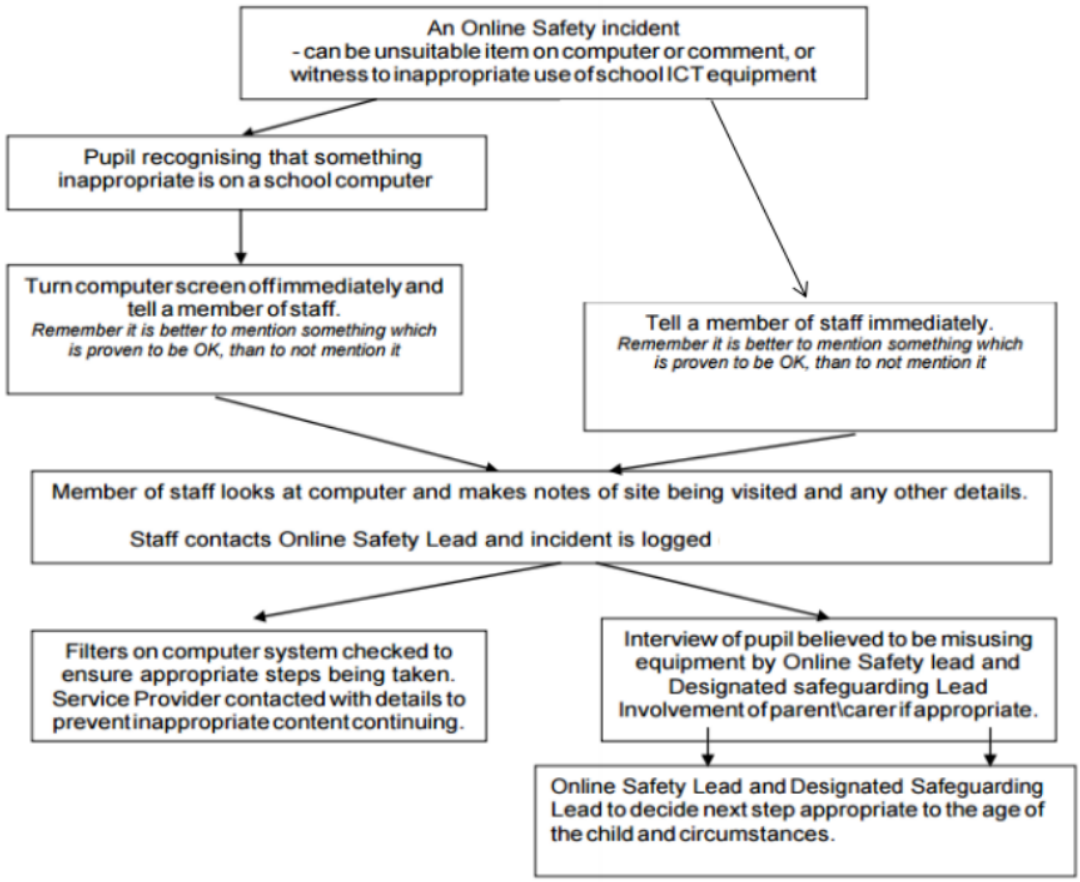
- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs 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.

Responding to Online Safety Incidents



Pupils have access to 'Self-referral' sheets which they can use to flag online safety incidents and outline what action they feel should be taken.

Please see Appendix 1.1 for an example of this.

The Online Safety Lead will be made aware of any incident of an online safety nature, and take appropriate steps to resolve and record the incident. All incidents relating to online safety are recorded using CPOMs by members of staff.

Appendix 1

Self-Referral Form

Name: _____

Class: _____

Date: _____

What happened?	
Where did it happen?	
When did it happen?	
How did it make you feel?	
What would you like done about it?	