Springfield Junior School

Online Safety Policy

Prepared by	*Scott Reynolds, Deputy Head*
Approved by the committee/Governing body	*March 2021*
Review date	*(Interim review September 2021)* *March 2022*

Online Safety at Springfield Junior School

At Springfield, we firmly believe that all staff has 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 endeavor 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.

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.

Safeguarding and Online Safety at Springfield Junior School

Our **Senior Designated Lead for Safeguarding** is **Mrs Louise Everitt** (Headteacher).

The **Alternate Senior Designated Leads** for Safeguarding are **Mr Scott Reynolds** (Deputy Headteacher), **Miss Beth Taylor**, **Miss Kim Cook** (Assistant Headteachers) and **Mr David Rycraft** (Family Support Worker).

Our **Online Safety Lead** is **Scott Reynolds** (Deputy Headteacher)

The **Computing Governor** is **Richard Smithson** and the **Safeguarding Governor is Samantha Green**.

What do we believe for 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.

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, has equal protection from all types of harm or abuse. Accessing a plethora of online platforms, our main objective is to support children with creating a positive digital footprint and make them aware of how to report concerns online.

Within school, our aim is to teach pupils the link between their own behavior when interacting in person, and also the behavior they display when online. We teach pupils that our digital footprint is something which still remains, unlike footprints on a sandy shoreline which can be washed away. Pupils are aware, and take responsibility, for their actions online.

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 were pupils can report concerns online, whatever the severity of the incident. As we all spend a greater number of hours online, we firmly believe that by promoting a culture of openness that children can have the confidence to report their concerns.

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 behavior 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 being discussed sporadically across the academic year. 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 online. 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.

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. During lessons, children are also taught about how to analyse websites and identify fake new; checking privacy settings on relevant apps they use; creating robust passwords; identifying scam emails; age restrictions for various apps; sharing content online and showing an awareness of copyright laws. In school, children are also promoted to be independent and autonomous learners. Self-referral sheets (see Appendix 1.0) 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 Online Safety Lead.

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.

Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils. Parents will also be directed to appropriate advice on this matter via the school website.

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 have access to report concerns in, or outside of school, by using self-referral forms. These can be found in all classrooms and are then provided to the Online Safety Lead.

-Workshops, in school or virtually, provide parents with practical tips to keep children safe online. External agencies, including the Neighbourhood Police Team, work in collaboration with staff in school to support all parents.

-Regular updates are provided to parents via Arbor or the school website (Online Safety) which provide up-to-date information about changes to online platforms and how to safeguarding pupils at home appropriately. The website also has an electronic form where parents can raise their own concerns and they are then sent to the Online Safety Lead.

-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.

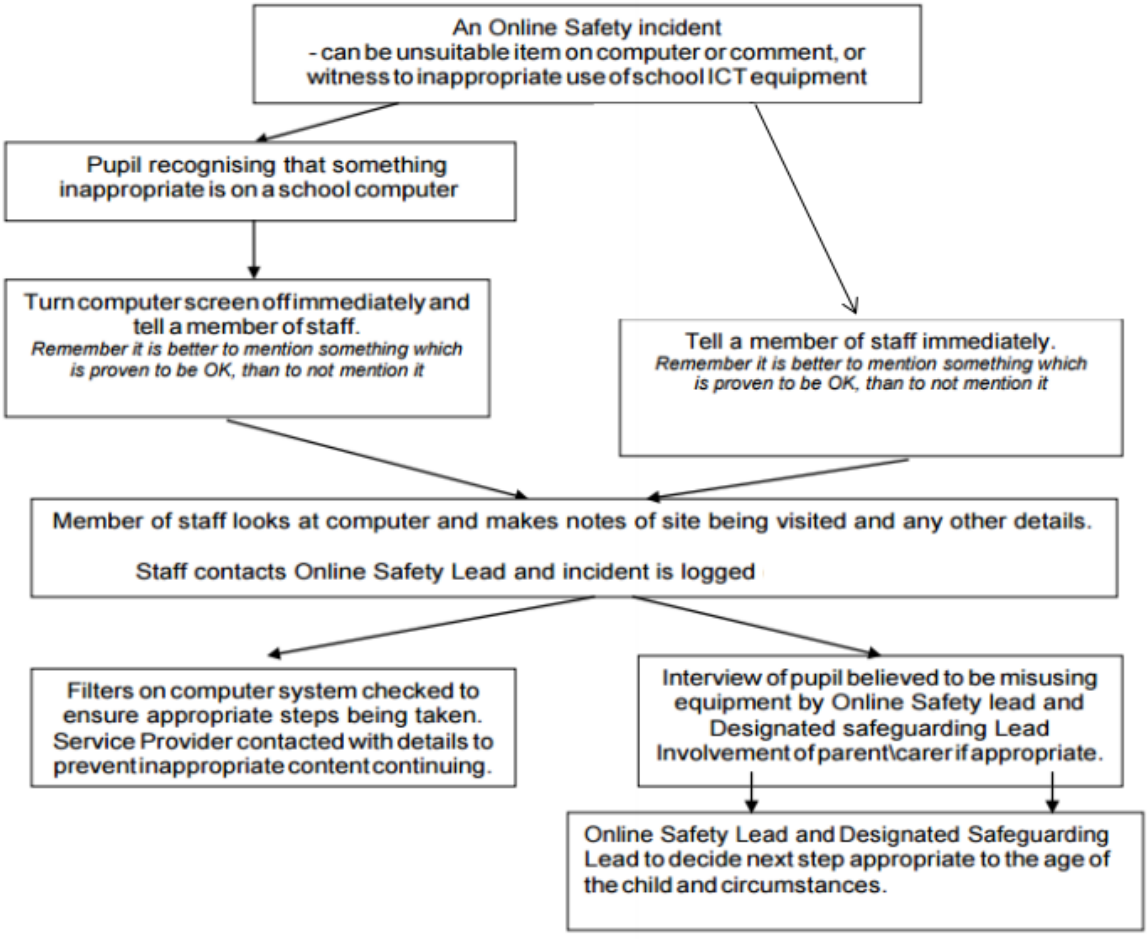
First names will only ever be published on the school website when celebrating pupils' learning. As part of Online Safety training, the school will not publish pupils' full names anywhere on a school website or other online space in association with photographs.

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 Scott Reynolds, Deputy Head.

Responding to Online Safety Incidents



Pupils also 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.

Computing Subject Lead

_____

Appendix 1.0

Self-Referral Form

Name: _____

Class: _____

Date: _____

SPRINGFIELD
JUNIOR SCHOOL

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