

# Springside School

## Online Safety Policy



November 2021

Approved by:	Governors - safeguarding	Date: November 2021
Last reviewed on:	November 2021	
Next review due by:	October 2022	

## Contents

1. Introduction and Aims .....	2
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating learners about online safety .....	5
5. Educating parents about online safety .....	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school .....	7
8. Learners using mobile devices in school .....	7
9. Staff using work devices outside school .....	8
10. How the school will respond to issues of misuse .....	8
11. Training.....	8
12. Monitoring arrangements .....	9
13. Links with other policies .....	9
14. Acknowledgements .....	9
Appendix 1: acceptable use agreement (learners and parents/carers) .....	10
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) .....	11
Appendix 3: online safety training needs – self audit for staff.....	12

---

## 1. Introduction and Aims

This policy has been written with the UN Convention on Rights of the Child in mind with particular reference to Article 3 (Best Interests of the Child), Article 16 (Children’s right to privacy’ and Article 17 (Children’s right to access to information from the media) which states:

*‘The best interests of children must be the primary concern in making decisions that affect them. All adults should do what is best for children. When adults make decisions, they should think about how their decisions will affect children. This particularly applies to budget, policy and law makers.’*

*‘Every child has the right to privacy. The law should protect the child’s private, family and home life, including protecting children from unlawful attacks that harm their reputation.’*

*‘Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.’*

Our school aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

### The 4 key categories of risk

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, anti-Semitism, 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 scam

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so.

## 3. Roles and responsibilities

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs (recorded using CPOMS) as provided by the designated safeguarding lead (DSL).

The governor who oversees Safeguarding (including online safety) is the Chair of Governors.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and the cognitive level of learners because of the importance of

recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

### **3.2 The headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### **3.3 The designated safeguarding lead**

Details of the school's DSL [and deputies 'DDSLs'] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DDSL takes operational responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT services and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

### **3.4 ICT Support Technician, Schools Broadband and Intelatech**

The ICT Support Technician in liaison with Schools Broadband and Intelatech are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

### **3.5 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that learners, as appropriate, follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure, if appropriate, their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating learners about online safety

At Springside, Online Safety is embedded within the PSHE curriculum. For learners it may be appropriate to teach PSHE as a discrete lesson. It is only included as an area of learning within the Investigative curriculum but, this is dictated by the cognitive level of the individual learner; therefore, if learners within any phase are at a cognitive level where it would be appropriate, it will be taught as a discrete lesson.

In all phases the core principles of PSHE and early objectives are taught, these are threaded through everyday activities, every area of learning and underpin every activity learners take part in.

Lessons will be taught according to the cognitive level of the learners, as decided by the class teacher in conjunction with Phase Leads. Teachers will plan for PSHE as taught sessions or within EYFS principles using, they will refer to the school's long-term plan and access the level of work as appropriate. Equals and the NSPCC programmes of study may be used. We will assess children at where they are and what they already know. We will use this to inform planning and next steps.

Should it be identified an individual required a bespoke programme of study or further support this will be provided. The school will utilise the class teams, phase leads, Therapeutic Inclusion workers, Wilderness Therapy workers and identified members of the leadership team.

Interventions are also available where it is felt a learner will benefit further from a bespoke package of support, these include Therapeutic Intervention (Th.Inc®); Wilderness Therapy and Behaviour Support Plans (BSP).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools

As appropriate to their cognitive understanding, learners 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

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

As appropriate to their cognitive understanding, by the **end of primary school**, learners 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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and the cognitive level of the learner.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and/or social media platforms. This policy will also be shared with parents.

Online safety will also be covered, as appropriate during parent progress meetings and EHC reviews.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the safeguarding team.

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

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

As dictated by the cognitive level of the learner; to help prevent cyber-bullying, we will ensure that learners who are able to, understand what it is and what to do if they become aware of it happening to them or others. We will ensure that those learners 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 will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

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 areas of learning where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets 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 will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, 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.

### 6.3 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 learners' 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\*

\* Staff may also confiscate devices for evidence to hand to the police, if a learner discloses that they are being abused and that this abuse includes an online element.

Any searching of learners will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

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

## 7. Acceptable use of the internet in school

All learners (or parents on their behalf), parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 learners, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

## 8. Learners using mobile devices in school

**Learners are not permitted to use personal devices in school unless specifically planned for educational purposes.**

Any use of mobile devices in school by learners must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.



## 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician and/ or the Online Safety Lead.

## 10. How the school will respond to issues of misuse

Where a learner misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and relevant safeguarding policies. 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 disciplinary procedures/ staff handbook. 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.

## 11. 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, safeguarding briefings and staff meetings).

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 learners can recognise dangers and risks in online activity and can weigh the risks up



- develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term

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.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. These are recorded using CPOMS.

This policy will be reviewed every year by the Online Safety Lead. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks learners face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-Bullying policy
- Staff disciplinary policy and procedures
- Staff Handbook
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy and agreements

## 14. Acknowledgements

Springside School would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- The Key School Leaders Support
- UK Safer Internet Centre
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

## Appendix 1: acceptable use agreement (learners and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

**Name of learner:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I will not:**

- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (learner):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet, and will make sure my child understands these as appropriate.

**Signed (parent/carer):**

**Date:**

## Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of learners without checking with teachers first
- Share confidential information about the school, its learners or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) or deputy designated safeguarding lead (DSL) know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that learners in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**Date:**

## Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways learners can abuse their peers online?	
Do you know what you must do if a learner approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for learners and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	