Somers Park Primary School
Statutory Policy required by other legislation

E-Safety Policy

Responsibility: Headteacher (SLT)

Agreed on:

Signed:

To be reviewed: September 2019

Contents

.....

1. Aims

Somers Park Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

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 as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Ed Clements

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 2)

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 designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead 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 manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 The Computing Coordinator

The Computing Coordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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

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 their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

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

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.

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. This policy will also be shared with parents.

Online safety will also be covered during parents' meetings.

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 DSL.

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

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will 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 will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. As part of our approach to PSHE and using the internet safely, class teachers will discuss cyber-bullying with their classes, and the issue will be 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 (see section 11 for more detail).

The school also sends information via school newsletters 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 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.

7. 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 (appendices 1 and 2). 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.

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

8. Pupils using mobile devices in school

Pupils may only bring mobile devices into school in exceptional circumstances with written permission, but are not permitted to use them during the school day and are stored securely in the school office.

9. Staff using work devices outside 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 2.

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 coordinator.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the disciplinary procedures set out in the school's behaviour policy. 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. 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, e-bulletins 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the Computing coordinator. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices (MET)
- Complaints procedure
- Code of Conduct

Appendix 1: acceptable use agreement (pupils)

EYFS AUP

Think before you click

S

I will only use the Internet and send messages with

A

I will only click on icons and links when I know

F

I will only send friendly and polite messages

E

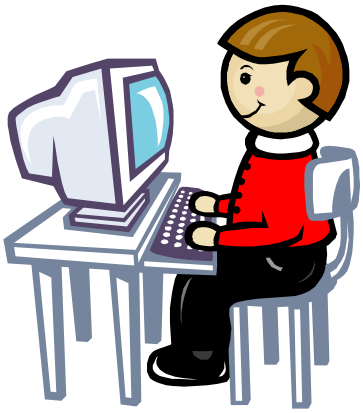
If I see something I don't like on a screen, I will always tell an adult

My Name:

Date:

KS1 - AUP

I want to feel safe on the computers all the time.



I agree that I will:

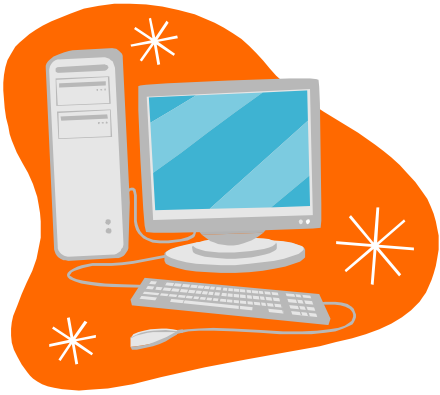
- always keep my passwords a secret
- only open pages which my teacher has said are safe
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email when I am at school
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself onto the computer
- never agree to meet a stranger
- never ask others for their personal details

Anything I do on the computer may be seen by someone else

Signed _____

Date _____

KS2 - AUP



When I am using the computer or other technologies,

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not open any attachments in e-mails without permission from an adult
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me
- ***I know that once I post a message or an item on the internet then it is completely out of my control.***
- ***I know that anything I write or say or any website that I visit may be being viewed by a responsible adult***

Signed _____ **Date:**_____

Staff and Volunteer Acceptable Use Policy

School Policy
This Acceptable Use Policy reflects the school online safety policy. The school will ensure that staff and volunteers will have access to technology to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy
This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally and professionally.

My Responsibilities
I agree to:
- read, understand, sign and act in accordance with the School online safety policy
- report any suspected misuse or concerns to the online safety leader
- monitor technology activity in lessons, extracurricular and extended school activities
- model the safe and effective use of technology
- demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

Education
I agree to:
- provide age-appropriate online safety learning opportunities as part of a progressive online safety curriculum
- respect copyright and educate the pupils to respect it as well

Training
I agree to:
- participate in online safety training
- request training if I identify an opportunity to improve my professional abilities

Online bullying
I agree to:
- ensure the school's zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying
- report any incidents of bullying in accordance with school procedures

Sexting
- I will secure and switch off any device discovered with an intimate sexting image and report immediately to the safeguarding lead.
- I will not investigate, delete or resend the image.

Prevent
- I will continually develop children's ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure
I understand that the school will monitor my use of computers and the internet. I will not try to by-pass any of the technical security measures that have been put in place by the school which include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media e.g. memory sticks (unless I have permission)

Passwords

- I will only use the passwords given to me
- I will never log another user onto the system using my login

Filtering

- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal and sensitive personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up and kept secure.
- If I believe there has been a loss of personal or sensitive data, I will immediately report it to the Data Protection officer in the school.

Use of digital images

- I will follow the school's policy on using digital images, especially in making sure that only those pupils whose parental permission has been given are published.
- I will not use personal devices for taking or sharing digital images within school without the direct permission of the Headteacher. Where permission has been given, I will ensure that all digital images relating to school are removed from my personal device at the earliest opportunity.

Communication

- I will be professional in all my communications and actions when using school technology systems.
- I understand that I need to be open and transparent in all my communications.

Email

- I will use the school provided email for all business matters.
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media and Personal Publishing

- I will ask permission before I use social media e.g. blogs, social networks or online communication tools with pupils or for other school related work.
- I will check with the SLT before I use sites/apps with learners to ensure that any pupil personal data is being held securely.
- I will follow the online safety policy concerning the personal use of social media.
- On any personal accounts I will not post any comments about any pupil and not post disparaging remarks about my employer/colleagues.

- When there is a Critical Incident, I will not post any comments online.

Mobile Phones

- I will not use my personal mobile phone during contact time with pupils.
- I will not use my personal mobile phone to contact pupils or parents.

Reporting incidents

- I will report any incidents relating to online safety to the online safety leader.
- I will make a note of any incidents in accordance with school procedures.

- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use technology and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School technology systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name

_____

Signed

_____

Date

_____

Appendix 2: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil 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 pupils 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? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**