Online Safety

POLICY

School Name
St. Andrew's Southgate

Updated
September 2022

To be reviewed
Sept 2024

Do justice,
love kindness
and walk humbly
with your God Micah 6.8

ST. ANDREW'S SOUTHGATE PRIMARY SCHOOL (CE) | 293 CHASE ROAD, SOUTHGATE, LONDON, N14 6JA

Internet/Online Safety Policy

St Andrew's school provides a safe, caring and inclusive Christian environment:

- Where self-esteem and mutual respect are encouraged through positive reinforcement and support;
- Where a broad and balanced education stimulates pupils enthusiasm and enjoyment of learning;
- Where skills are developed for learning in the present, and as a foundation for the future;
- Where everyone is given the opportunity to develop their full potential.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's online safety policy will operate in conjunction with the curriculum and other policies including those for Behaviour, Bullying, Data Protection and Code of Conduct.

Good Habits

- Online Safety depends on effective practice at a number of levels:
- Responsible IT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

We know pupils will use the Internet outside school. They will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries; inclusion in the London Grid for Learning which connects all London schools; educational and cultural exchanges between pupils world-wide;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations; improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and the DfE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access is designed for pupil use and includes 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.
- Each term, children will learn about how to be safe online.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- All staff must read and sign the 'Code of Conduct' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the SLT.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Social Networking

- Schools should block/filter access to social networking sites unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, LGfL and the Internet Service Provider to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras/cameras in tablets which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children are only allowed to bring mobile phones to school if they walk to/from school on their own. Written permission from parents is required. Children must hand them in to the school office staff every morning and devices are collected at home time.

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupils is being compromised.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images

- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs and video of pupils are published on the school Web site.

Information System Security

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enfield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit IT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate.

Handling Online safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Each class to have an online safety display promoting how to stay safe online
- Online safety to be taught through the school's IT curriculum Kapow

Staff

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of Online safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site. The school will also organise Online safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Computer games

St Andrew's School understands the importance of age appropriate viewing and playing of computer games and the risk exposure to sexual and violent game play poses to children. If we are made aware of pupils playing games that are age inappropriate for them we will contact the parents and if necessary contact the police to ensure access to the games is stopped.

School Online Safety Policy

The ICT lead also promotes the teaching of online Safety across the school . They will inform one of the safeguarding team in the event of an online incident. This will be logged using the school's safeguarding system called My Concern and overseen by the HT or DHT.

Policy reviewed Sept 2022

The Online Safety Policy will be reviewed bi-annually. This policy will next be reviewed in October 2024.

Appendix A –Changes to KCSIE 2022/23

Appendix B - Referral Process for responding to Online safety incidents in school

Appendix C - Online Safety Rules

Appendix D Letter to Parents

Appendix E Information and Communications Technology

Acceptable use of Internet Agreement

Appendix A

Online Safety within 'Keeping Children Safe in Education' 2022

On the 6th July 2021 the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 1st September 2022. Schools and Colleges must comply with KCSIE 2021 until that date.

KCSIE is statutory guidance and all schools and colleges must have regard to it when carrying out their safeguarding. The DfE use the terms "must" and "should" throughout the guidance; "must" is used when the person in question is legally required to do something and "should" when the advice set out should be followed unless there is good reason not to.

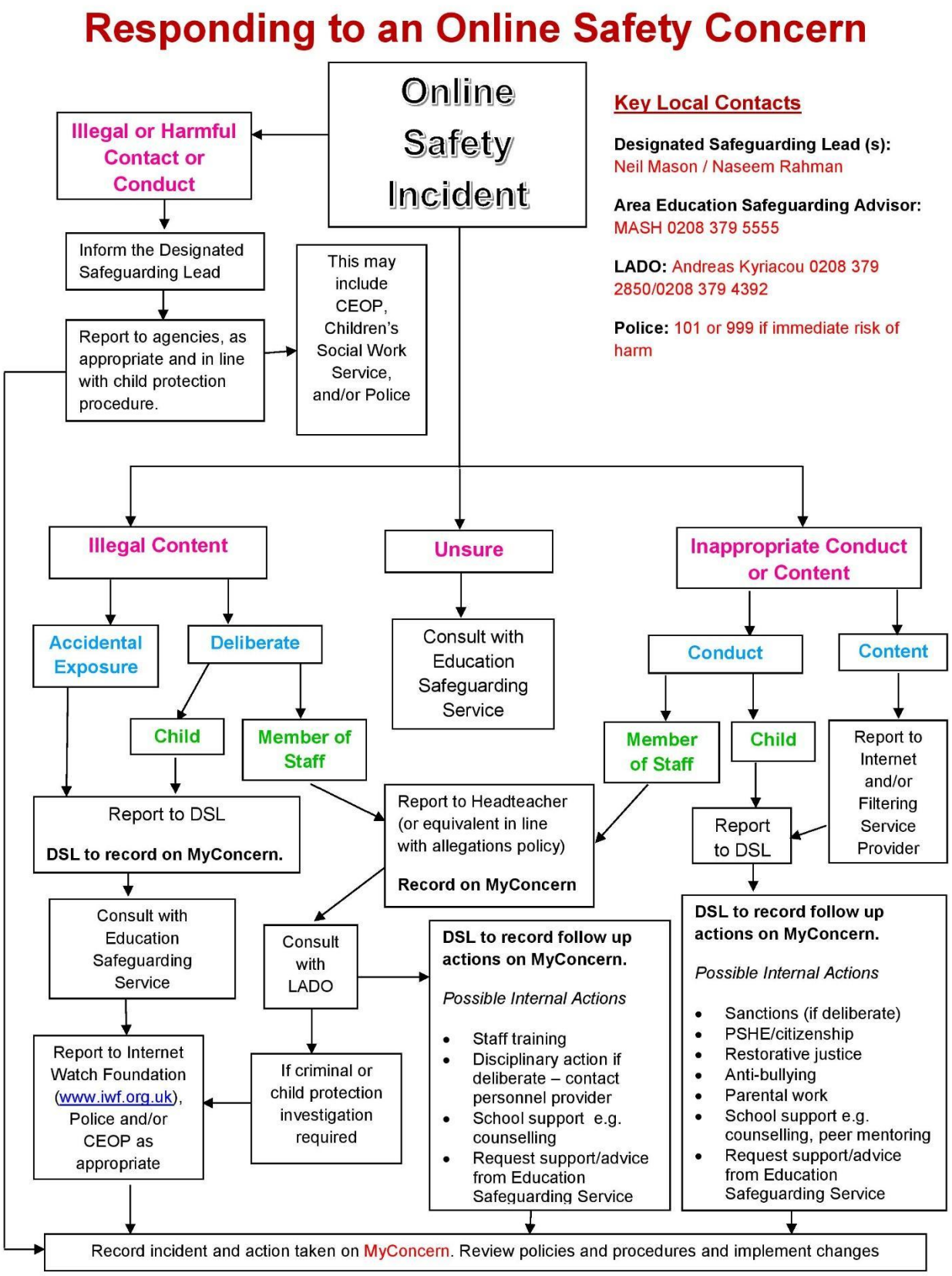
This document only focuses on elements of KCSIE 2022 relevant to online safety. Designated Safeguarding Leads (DSLs) and leaders should read the entire document when evaluating their wider safeguarding practice.

- Specific online safety content has been added and strengthened in part two to ensure online safety is viewed as part of a school/college's statutory safeguarding responsibilities.
- The standalone annex on online safety (Annex D in KCSIE 2021) has been removed and content is now fully integrated in part two and in annex B/C.
- Peer on peer abuse has been amended to 'child-on-child' abuse throughout.
- Part two has been updated to signpost DSLs and school/college leaders to the DfE 'Harmful online challenges and online hoaxes'
- All governors and trustees should receive appropriate online safety information/training as part of their safeguarding and child protection training; this should be received as part of their induction and be regularly updated.
- Governors/trustees should ensure that the school/college leadership team and relevant staff 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.
- New content has been added to part two to recognise the importance of schools/colleges communicating regularly with parents to reinforce the importance of children being safe online.
- A new paragraph has been added to part three to suggest that as part of the shortlisting process, schools and colleges should consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/college might want to explore with applicants at interview.
- Part five has been re-written to incorporate the previously standalone DfE sexual violence and sexual harassment guidance; it is important DSLs are aware of the additional content now included in part five.

• Annex D contains updated links to online safety resources to support schools and colleges.

Appendix B

Flowchart for responding to Online safety incidents in school



Appendix C

KS1 ONLINE SAFETY RULES

THINK THEN CLICK

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

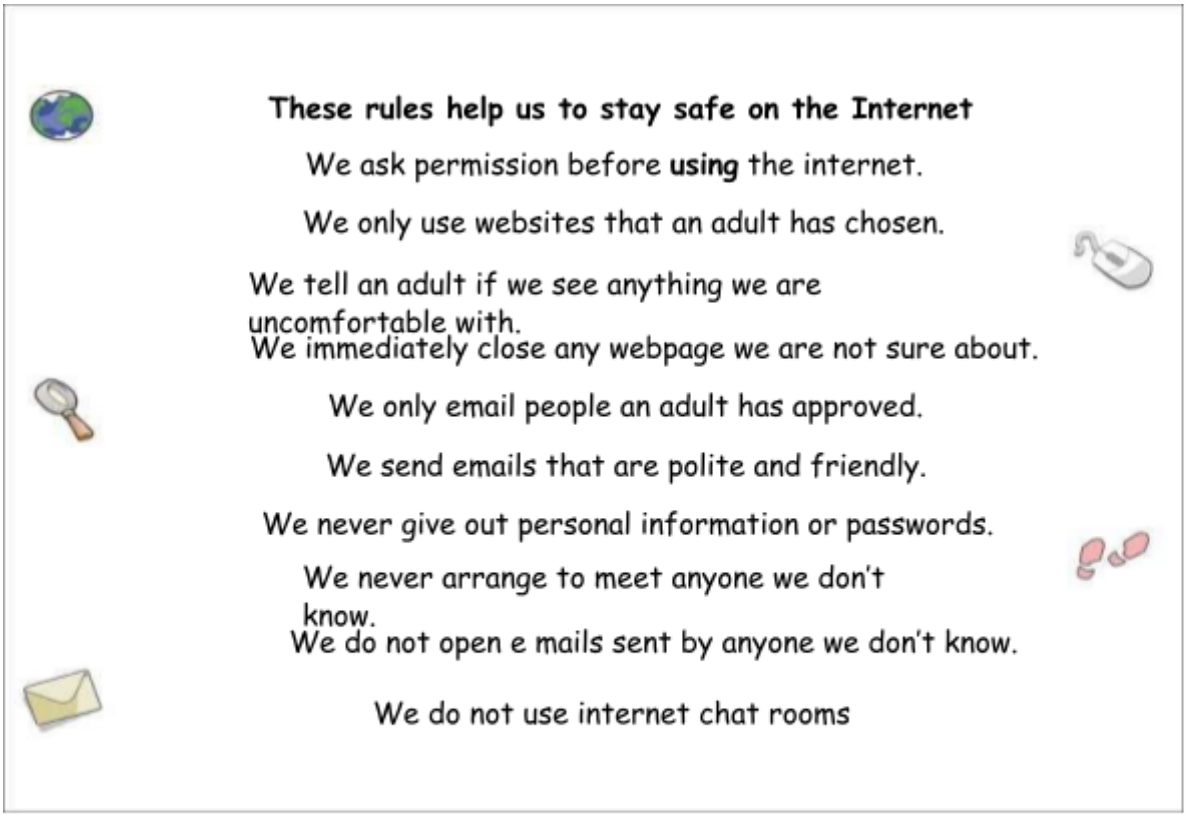
We can click on the buttons or links when we know what they do.

We can search the Internet with an adult. We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

KS2 ONLINE SAFETY RULES



Online safety Rules

These Online safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Appendix D - Letter to parents

London Borough of Enfield

ST. ANDREW'S SOUTHGATE PRIMARY SCHOOL (CE)

Head Teacher: Mr N Mason BA (Hons)

297 Chase Road ■ Southgate ■ London N14 6JA ■ Tel: 020 8886 3379 ■ Fax: 020 8886 1231
e: office@st-andrews-southgate.enfield.sch.uk ■ www.st-andrews-southgate.enfield.sch.uk

October 2022

Dear Parents/Carers

Information and Communications Technology

As part of our computing scheme of work and general curriculum enhancement, St Andrew's Southgate Primary School is providing supervised access to the internet. We are confident that this will benefit our children and equip them with important skills and knowledge in the wider world.

Our internet service provider, overseen by Enfield LA, operates a filtering system that restricts access to inappropriate material. Children will always be supervised when using the internet, and the rules of responsible internet use will be explained to them at school.

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

To support the policy, we ask you to sign the agreement overleaf. It would be helpful also if you would talk to your child about the 'rules' whenever necessary. Should you wish to discuss this agreement or any aspect of the Internet use, please contact me to arrange an appointment.

Yours faithfully

Mr Neil Mason

Head Teacher

Appendix E

ST ANDREW'S SOUTHGATE PRIMARY SCHOOL (CE) 2022-23

COMPUTERS - PUPIL ACCEPTABLE USE POLICY

J
2020/21

At St Andrew's Southgate Primary School we appreciate the role that computers can play in enhancing our children's education. However, we are also mindful that computers must be used in a sensible manner. All pupils must adhere to the following rules when using school computers:

If these rules are not followed, pupils may find:

- They are not allowed to use the school computers
- They can only use the computers whilst being more closely supervised.

Staff at St Andrew's Southgate Primary School will ensure that children are shown how to use the computers.

Rules

I will only use polite language when using computers

✔ I will not write anything that may upset someone

✔ I know that my teacher will regularly check what I have done on the school computers

✔ I know that I should not tell anyone my name, where I live or my telephone number over the internet

✔ I must not tell my usernames or passwords to anyone except my parents

✔ I must log off after I have finished working on the computer

✔ I must not use the computers in a way that stops other people using them

✔ I will report any website that makes me feel uncomfortable to the teacher

✔ I will tell my teacher if I receive any messages that make me feel uncomfortable

✔ I will take care of the equipment and the work of another person on a computer

✔ If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

Pupil Acceptable Use Policy

I have read the school rules concerning using the school computers. I will used the computers sensibly and follow these rules and the instructions of my teacher.

✔ I agree to report anyone not using the computers sensibly to my teacher.

✔ I agree to tell my teacher if I see websites that make me feel unhappy or uncomfortable.

✔ I understand that if I do not follow these rules, this will mean that I might not be able to use the computers.

Pupil Name

Parent/Carer Name Parent/Carer Signature

Date: