E Safety Policy

Excellence for All

Policy reviewed/updated	September 2025
Next update	July 2027
Committee	Quality of Education
Interim Executive Headteachers	Mr Ben Waldram and Mrs Lynne Orme
Chairs of Governors	Mrs Karen Shead and Mrs Clare Colmore

Revision date	Author of changes	Summary of changes

If you have any concerns about safeguarding, please contact us on the email below or scan the code to see the safeguarding page on our website.
dsl@snapewood.nottingham.sch.uk

In the 21st century, "being online is an integral part of children and young people's lives" (NSPCC). Whilst the online world can be an incredible place that is useful to teaching and learning, at Snape Wood we recognise the potential threats that social media, apps, games, websites and software can pose on our whole-school community.

The aims of this policy:

- To reflect the importance of Online Safety across school.
- To make clear the systems and procedures we have in place.
- To ensure all members of our school community share responsibility for the teaching of Online Safety.

This Policy is to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. The policy will operate in conjunction with other policies including those for Computing, Student Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security. The role of e-safety will be overseen by the Computing lead in conjunction with the designated Safeguarding leads, but ultimately, it is a shared responsibility by **all staff** at Snape Wood Primary School.

1. Roles and Responsibilities

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 headteacher

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

The Designated Safeguarding Lead (DSL)

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, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- 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
- Liaising with other agencies and/or external services if necessary
- In partnership with the Computing Lead, provide regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

The Computing Lead/ Schools IT

The Computing Lead should work with Schools IT to ensure:

- Appropriate filtering and monitoring systems are in place, 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
- That the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- A full security check and monitoring of the school's ICT systems is conducted on a [regular basis.
- Access to potentially dangerous sites is blocked and, where possible, preventing the downloading of potentially dangerous files.
- That any online safety incidents are logged, reported to the DSL and dealt with appropriately in line with this policy.
- That any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Additional Section on Filtering & Monitoring (in light of changes to KCSIE 2023)

Information Monitoring and Filtering

Introduction

This section on filtering and monitoring outlines the guidelines and procedures for monitoring and filtering information accessed by students, staff, and visitors within Snape Wood Primary school. The policy aims to ensure a safe and secure learning environment while promoting responsible and appropriate use of digital resources.

Purpose

The purpose of this section within our E-Safety Policy is to:

a. Safeguard students from accessing harmful or inappropriate content.

b. Protect the school's network and computer systems from security threats.

c. Encourage responsible and ethical use of digital resources.

d. Comply with relevant legal and regulatory requirements.

Responsibilities

a. School Administration: The school administration is responsible for implementing and enforcing this policy, including selecting and maintaining appropriate filtering and monitoring tools, and providing necessary training to staff.

b. Staff: Staff members must promote responsible and safe use of digital resources, monitor students' online activities during school hours, and report any concerns or incidents to the appropriate authorities.

c. Students: Students must use digital resources responsibly and follow the school's guidelines for acceptable online behaviour. They should report any inappropriate content they come across to their teacher or a trusted adult.

Filtering and Monitoring Tools

a. The school will implement appropriate filtering and monitoring tools to restrict access to websites and content that are deemed inappropriate, harmful, or unrelated to educational purposes. For this purpose we use staff vigilance / Impero / Apple Classroom and currently the school is looking into Smoothwall software.

b. The filtering system will be regularly updated and configured to block or filter categories such as violence, explicit content, gambling, hate speech, and other potentially harmful materials.

c. The school will also implement monitoring tools to monitor students' online activities, which may include tracking websites visited, search queries, and email communications. This monitoring will be conducted in compliance with applicable privacy laws and regulations.

Acceptable Use and Online Behaviour

a. The school will provide clear guidelines to students and staff regarding acceptable use of digital resources, including rules on accessing and sharing appropriate content, cyberbullying, online privacy, and copyright infringement.

b. Students and staff are expected to use digital resources in a responsible, respectful, and ethical manner.

c. Online communication, including email and social media use, should be conducted professionally and responsibly, with appropriate language and tone.

Reporting and Response Procedures

a. Staff members should promptly report any concerns or incidents related to inappropriate or harmful content to the designated authority within the school, such as the designated safeguarding lead.

b. Reported incidents will be thoroughly investigated, and appropriate actions will be taken to address the situation, which may include parental involvement, disciplinary actions, or involvement of external authorities if necessary.

c. Students, staff, and parents should be encouraged to report any potential breaches of this policy or incidents they come across.

Training and Education

a. The school will provide regular training and education sessions for staff, students, and parents to raise awareness about safe and responsible use of digital resources, including the potential risks and consequences associated with inappropriate behaviour online.

b. Training will also cover identifying and reporting online safety concerns, understanding the importance of privacy and data protection, and promoting positive digital citizenship.

Review and Amendments

a. This policy will be reviewed periodically to ensure its effectiveness and compliance with legal and regulatory requirements.

b. Amendments to the policy may be made as necessary, with proper communication and training provided to staff, students, and parents.

c. Feedback and suggestions from stakeholders will be considered during the policy review process.

Policy Dissemination

a. This policy will be communicated to all staff, students, and parents, and a copy will be made available on the school's website.

b. Any updates or changes to the policy will be promptly communicated to relevant stakeholders.

c. Acknowledgment of receipt and understanding of this policy may be required from staff, students, and parents.

Compliance

a. Failure to comply with this policy may result in disciplinary action, which may include restricted access to digital resources, loss of privileges, or other appropriate measures.

b. Breaches of this policy may also result in the involvement of external authorities, as required by law.

Conclusion

This Information Monitoring and Filtering Policy aims to create a safe and secure online environment for students, staff, and visitors within UK primary schools. By promoting responsible and ethical use of digital resources and implementing appropriate filtering and monitoring measures, the policy ensures that students can access educational content while protecting them from potentially harmful or inappropriate material.

(This list is not intended to be exhaustive.)

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 and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

Parents

Parents are expected to notify a member of staff or the headteacher of any concerns or queries regarding this policy.

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.

2. Teaching and Learning

Key messages around internet safety will be clearly displayed around school, particularly in the Digital Zone and in classrooms. At the start of every school year, children in all classes must sign the Class Contract to show that they understand the school's stance. Every year, we will participate in @National Online Safety Week" with all classes engaging in activities and essential learning. Where possible, parents will be invited into school to support this.

In line with the current National Curriculum and objectives within our Root and Branch document:

Pupils in Key Stage 1 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

Using Google's scheme "Be Internet Legends", 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

Why Internet use is important

- The Internet is an essential part of our lives in the 21st century for education, business and social interaction. As a school, we have a duty to provide children with high-quality Internet access as part of their learning experience across the curriculum. Internet use is a part of the statutory curriculum and a vital tool for both staff and pupils on a daily basis.
- Pupils use the Internet widely outside school and will need to be taught how to the internet can be used (Year 1), how to use it safely (Year 3) and how evaluate the reliability of various Internet sources (Year 4) in order to take care of their own safety and security.

Internet use will enhance learning

- At Robin Hood, we feel passionate about the use of technology to enhance teaching and learning, making excellent use of our Digital Zone, 1:1 iPads and classroom-based laptops. Children will have regular access to the Internet and therefore our Internet is designed for pupil use, with filtering made appropriate
- Through our updated curriculum, children will be taught the difference between acceptable and unacceptable use where the Internet is concerned (Year 3) and will be given clear objectives for Internet use.
- Internet access will be planned carefully to enrich and extend learning activities. Staff should guide pupils in online activities that will support the 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.
- Pupils will be taught how to evaluate Internet content. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Staff can use the root and branch document (2020) to use age-appropriate Digital Literacy objectives when delivering lessons that make use of the Internet.

3. Management of internet and devices.

- Schools IT provide high levels of web filtering to ensure only appropriate content is viewed. Staff can access a local deny list if inappropriate websites are reported.
- School IT systems capacity and security are reviewed regularly. Snape Wood will work with Schools IT to ensure that systems are reviewed and improved to better protect our children (e.g. annual health check)
- Virus protection will be updated regularly.
- Security strategies will be discussed with NG computers (in house technicians).
- iPads across school are managed by KRCS and apps are deployed using the managed service, with permission from the Computing Lead. Apps must only be deployed if they are beneficial to teaching and/or learning.
- iPads may be used to AirDrop documents or photographs between children and teachers but this must, at all times, be for teaching and learning purposes only.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing Lead to deal with accordingly.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time by either children or staff. The sending of abusive or inappropriate text messages is forbidden and children should be encouraged to report this to a parent or a member of staff so that it can be dealt with in-line with school policy.

- Staff will be issued with a school phone and charger for use on school trips and residential trips. This must be returned to the school office upon return.

4. Personal data

- As a school, we must follow current GDPR guidelines.
- Parents will complete forms when their child joins Robin Hood, giving permission to share data.
- Any data breaches must be recorded to our DPO immediately.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

5. School Website and Social Media

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.
- Staff have a shared expectation for editing and updating of class pages on the website and therefore have a responsibility for ensuring the content uploaded is accurate, appropriate and in-line with the GDPR regulations.
- Photographs that include pupils will be selected carefully and only used if parents have given the relevant permission for the publication of photographs.
- Pupils' names will not be used in association with photographs.
- The school admission form contains a section for parents/carers to sign to give permission for photographs of pupils to be published on the school website, on social media and for further platforms (e.g. newspapers, Nottingham Music Hub).
- Access within school to social networking sites is blocked/filtered by Schools IT.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be reminded that the use of social network spaces outside school is inappropriate for primary aged pupils. This message will be made clear should any issues concerning children arise outside of schools.

<u>Assessing risks</u>
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Nottingham City LA can accept liability for the material accessed, or any consequences of Internet access. To ensure unsuitable is not viewed the school will implement the following measures;

- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective;
- The use of computer systems without permission or for inappropriate purposes could lead to disciplinary action;
- Methods to identify, assess and minimise risks will be reviewed regularly.

6. Email

- Email is essential for staff to communicate with each other. Staff are given an email address upon joining Snape Wood and passwords for these must be kept private at all times.
- Staff must behave professional and appropriately at all times when using email. Any emails deemed to be inappropriate must be reported to the head teacher.
- Schools IT will alert all staff if there are any concerns around spam emails and will inform staff with the appropriate measures needed if they have become a victim of spam or other technical issues.
- Following our Remote Learning and Communications plan in 2020, parents have access to staff email addresses. This communication must remain professional at all times. Any concerns regarding the content or misuse of this email system must be passed onto the headteacher immediately.
- The forwarding of chain letters is not permitted.

7. Communication

Communication is deemed to be very important between all members of our whole-school community at Robin Hood, therefore is it imperative that we are clear on the following messages to ensure our policy is implemented and followed effectively.

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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents and pupils will need to work in partnership with staff to resolve issues. All matters will be dealt with promptly and sensitively

Parental involvement

- All parents will have access to our E-Safety policy via the school website and can request a printed copy at the office.
- Parents will be regularly updated with online safety-related messages in our dedicated termly newsletter, produced by the Computing Lead. This will be sent out to all parents via ParentPay and also uploaded to the school website and Twitter page.
- As mentioned, parents have access to staff emails addresses and will be reminded how to behave when contacting a child's class teacher. This is made clear on the school's communication plan.
- Where parents are contacted via Marvellous Me, staff will use this app for its intended purpose only. Any concerns around misuse must be reported to the headteacher to deal with in line with this policy.

Showbie

- Children who access 1:1 iPad provision have an account on Showbie. These accounts must be used for teaching and learning purposes only and children should be taught how to access and upload work safely.
- In the event of Remote Learning, staff are permitted to communicate with pupils via Showbie, using the whole-class discussion page or through commenting on children's work. Written or voice recorded comments are permitted.

8. Staff training

- Where appropriate, staff will be made aware of any updates either from the Computing Lead or Safeguarding lead.

- The Computing lead will feedback to staff with any important messages that arise in training he/she attends, which could benefit the wider-school community.
- Regular training and updates may be given through staff meetings led by the Computing Lead. Some sessions may be offered throughout the year from external providers or other local schools.
- Staff will require high-quality training where new devices or software is purchased so that this can be used effectively, modelling appropriate use to children, parents and other staff members.
- As part of our shared responsibility around online safety, all staff have a duty to stay up to date or at least have some awareness of online safety messages which may reach the news or social media platforms, particularly where these may affect our children (e.g. what is trending online).

9. Legislation and guidance for schools

It is vitally important that school staff stay up to date with current thinking and legislation around safeguarding children, where online safety is involved. These documents and websites will provide further guidance for the whole-school community. Much of this policy is based on the Department for Education's (DfE) statutory guidance.

- Keeping Children Safe in Education
- Cyber-bullying: Advice for headteachers and school staff
- Teaching Online Safety in Schools
- NSPCC: e-Safety for schools
- National Online Safety
- 'Gotta Be Safe Online' section of the school website.

10. Links to other policies

This e-Safety policy is linked to our:

- Child protection and Safeguarding policy.
- Behaviour policy.
- Staff disciplinary policy.
- Data protection policy and privacy notices.
- Complaints procedure.
- Acceptable Use policy.
- Computing curriculum.