



E Safety / Online Policy

Online Safety is an important part of keeping children safe at Nun Monkton School. We have extensive security measures in place in school to help safeguard pupils from potential dangers or unsuitable material. Online safety is explicitly taught in all year groups. Our aim is that all children at our school will understand how to use the internet effectively and responsibly, and how to stay safe when accessing the internet, both at school and at home.

Online Safety in school is overseen by the Headteacher and supported by the Computing Lead Teacher. This policy should be read in conjunction with the Safeguarding & Child Protection Policy and the Information (Data Protection) Policy which can be found on our website.

Rationale

The internet and other digital technologies run through all aspects of life in a modern technological society and develop at pace, which is part of everyday life in education, business and social interaction. Although many of our pupils here at Nun Monkton do not use such ICT outside of school, they see others in their households doing so and have access to it. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. Every pupil is entitled to have access to the internet and digital technologies, in order to enrich their learning. Similarly, at home, many children have access to a range of technologies and it is part of the responsibility of school, alongside parents, to help to educate children in how to stay safe.

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- a) The Internet
- b) E-mail
- c) Music download sites
- d) Gaming Sites
- e) Mobile phones with camera and video functionality
- f) Phones with email, web functionality
- g) Instant messaging – often using web cams
- h) Social networking sites
- i) Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- j) Blogs
- k) Video broadcasting sites
- l) Chat Rooms

Who does the policy apply to?

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

Overall aim

Our overall aim is that all children at our school will understand how to use the internet effectively **and** how to stay safe when accessing the internet, both at school and at home.

Objectives

All children at our school should learn:

- that the internet contains an almost infinite amount of information which, when used appropriately, can be educational and entertaining.
- that the internet is a powerful tool for communication which allows us to be in instant contact with people from all over the world.
- that most of the information on the internet is not verified and therefore has to be checked for accuracy.

- that there is some content on the internet which is inappropriate or even illegal and should be avoided.
- that some people misuse the internet to communicate unkind or hateful messages (including cyber bullying) and that these people should be reported.
- that some people on the internet are not who they say they are.
- that a small number of people want to hurt children and could use the internet to make contact with them.
- how (or who) to report content or messages that are inappropriate, harmful or upsetting.
- that harmful and upsetting behaviour online may affect their mental health and that, if this should occur, they know who to speak to.

Through computing, PSHE and subject lessons, pupils will develop an understanding of the uses, importance and limitations of finding information on the internet.

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate the information they find on the internet.
- Pupils will develop a positive attitude to using the internet and develop their Computing capability through both independent and collaborative working.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.
- Pupils will be taught how to report inappropriate web content.

Through computing and subject lessons, pupils will develop an understanding of how to use the internet to communicate safely and appropriately.

- Pupils will be taught not to share passwords or personal information.
- Pupils will be taught how to use email/messages effectively, including checking for bogus messages.
- Older pupils will be taught how to share information using collaborative tools, including Google Workspace, and how to comment on other people's posts appropriately.
- Pupils will be taught how to respond to inappropriate comments (cyber bullying). Who to speak to or contact if they experience this.
- Pupils will be taught how to respond to unsolicited attention.

How we teach online safety at our school

E-Safety/Online Safety is part of the National Curriculum for Computing. It is explicitly taught in all year groups as part of the Computing curriculum within the six themes of computing teaching throughout each year. Children will also be taught about e safety in PSHE lessons, within general day to day use of ICT equipment for a range of learning activities and if a member of staff feels a particular aspect of e safety needs focus within their class (sometime but not exclusively in response to something that has happened in school or at home).

Children, staff and visitors are all made aware of our 'Safe Use of the Internet Guidelines'. Guidelines will be displayed in the school on classroom walls. E-Safety information is also contained within staff training and available on the school website.

In class, staff model good internet practices and etiquette.

To complement our teaching, staff may use resources from many sources including (but not exclusive to) the following websites and support networks:

BBC Bitesize <https://www.bbc.com/ownit>

CEOP Education – e-safety <https://www.thinkuknow.co.uk/>

[Parents and Carers resource sheet | Childnet](#)

[Primary online safety for teachers](#)

www.digizen.org (Useful information for parents and teachers)

<https://nationalonlinesafety.com/> (Useful information for parents and teachers)

Coding and e-safety <https://studio.code.org>

Other ways we support E safety in our school

- A monthly Online Safety newsletter is sent to parents/carers and put on the school website in the 'News' section. There are also online safety videos to access from the same website.
- A useful e safety/information update is regularly included in the Headteacher's newsletter to parents.
- Useful information or links to helpful organisations for parents are regularly updated on the school's website
- All staff and any visitors who will be involved in using IT equipment in school will sign the school's IT acceptable use agreement

Mobile Phones and other handheld technology

Pupils are not permitted to have mobile phones or other personal handheld technology in school.

In exceptional circumstances, and only with the prior agreement of the Headteacher, a child may be permitted to have a phone in school. If this is the case, the phones must be switched off and handed to the school office who stores them safely before handing back at the end of the day.

Monitoring

- A variety of monitoring strategies are in place to minimise safeguarding risks on internet connected devices and include the following:
- Our internet provision currently utilises the Smoothwall filtering solution. This is a comprehensive filtering platform designed to protect schools from inappropriate on-line content, including new requirements around child safety/anti radicalisation, as well as meeting or exceeding the current compliance and recommended safeguarding children legislation. Detailed alerts and reporting are configured to alert of an incident at a school, enabling a fast response to ensure children's safety.
- Children at our School do not have unsupervised access to the internet in school, and staff ensure children are appropriately monitored when using the internet.
- Smoothwall provides network monitoring, using log files of internet traffic and web access. It restricts what children (and adults) can access on the internet, to reduce the risk of exposure to inappropriate content/platforms. It keeps a log of what users access on the internet as well as blocking content and categories of content.
- Children are physically monitored by staff watching screens. Children are not left unattended whilst using devices in school.
- No system is fool proof, and it is important to not be lulled into a false sense of security. This is why we explicitly teach the children that the school filtering system is designed to stop them seeing inappropriate content but that no system is perfect - so we also teach them what to do if something online makes them worried/scared/uncomfortable i.e. to tell a trusted adult so we can both support the child, and get the system improved.
- The staff have responsibility to report any breaches to the Headteacher/DSL or the DSL and also to make the Computing Lead aware.

Reporting

All incidents or disclosures will be treated with the utmost care and diligence. Children making disclosures will be given the opportunity to say what they need in a safe space, with no leading questions. However, they will also be told that a member of staff cannot keep their disclosure secret and will have to inform another member of staff. All disclosures should be recorded on 'My Concern' and brought to the Headteacher's/DSL's attention. The school's safeguarding policy will then be followed.

Apparent or actual misuse or illegal activity could include:

- child sexual abuse images
- 'sexting'
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- inappropriate messages or online bullying (mobile phones, social media, email etc.)
- other criminal conduct, activity or materials e.g. county lines evidence/ FGM etc.

The Headteacher or other authorised adult would contact NYES Digital for their advice and assistance in investigating the breach and what steps to take in terms of the ICT and Smoothwall systems.

The Headteacher / DSL meets regularly with the School's Safeguarding Governor. Amongst the things that are focused on is the effectiveness of the filtering and monitoring systems and rigorous supervised tests of the system are carried out at least termly

This policy supports our school aims to:

- Enable children to become **independent** and **confident** learners; **well-rounded** characters who are **self-aware**, **reflective** and **resilient** individuals.
- **Care for and about each other**, be **courteous** and **empathetic**, showing **respect** and **understanding** towards everyone.
- Create a **safe and stimulating** place where children are **happy** and **enthusiastic** learners, where they learn how to keep themselves **safe and healthy**, able to **communicate** & work in a **team**, developing **confidence** and **life skills** together.
- Encourage everyone to have **high expectations** of **themselves and others**, **supporting** and **challenging** everyone to **achieve** their best, developing a strong **work ethic**, **self-motivation** and taking **pride** in their achievements.
- Enable children to develop an **understanding of the wider world** through learning and exposure to a **variety of cultures**, **ideas** and **beliefs**, **respecting** and **recognising individuality** and **diversity**.
- Provide a **wide range of interesting and exciting learning opportunities** to **enthuse** everyone to be lifelong learners, through engagement in a curriculum that instils **values for life** and **prepares pupils** for wherever their journey takes them as adults.

Date: June 2025

Policy to be reviewed in June 26

BE SMART ONLINE



S

SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.



M

MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

THINK
U
KNOW
CO.UK

A

ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.



R

RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.



T

TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk





BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.



APPENDIX 2 – information for parents

Parents and Carers Key Online Safety Resources



Childnet have a dedicated area to support parents and carers with information on key topics, advice and activities to share with your child. childnet.com/parents-and-carers

Childnet Resource Hub

Choose resources for 'parents and carers' to see leaflets, resources and activities to do with your child. childnet.com/resources



Advice on key online issues, tips, guides and blogs from partners: Childnet, SWGfL and the IWF. saferinternet.org.uk

Safer Internet Day

Join the celebrations for Safer Internet Day every February! We provide free tips, advice, videos, quizzes and more. saferinternetday.org.uk

Want to stay up to date? Sign up for the Childnet newsletter to hear about our latest advice on the most popular apps, new blogs and more. childnet.com/signup

Reviews and tools

The Family Gaming Database shares research and advice on thousands of video games, including content warnings and PEGI ratings. familygamingdatabase.com

Common Sense Media provides expert reviews, advice and age-appropriate recommendations on games, apps, films and more. Users can access up to three free reviews per month. commonsensemedia.org

Parental controls and privacy settings described step-by-step alongside support on a range of online safety topics. internetmatters.org/parental-controls

Making a report

For advice on the reporting tools for popular games, apps and social media platforms visit childnet.com/how-to-report for more information.

Report Harmful Content is a national reporting centre offering advice and links to industry reporting tools. It also provides support by reviewing outcomes after a report has been made on a platform or app. reportharmfulcontent.com

Report suspected online child sexual abuse or grooming to your child's school/local police. If necessary, contact the **Child Exploitation and Online Protection command (CEOP)**. ceop.police.uk

Report online child sexual abuse images and videos with the **Internet Watch Foundation's** anonymous reporting tool. iwf.org.uk

Information on hate crime and advice on how to report it in England, Wales and Northern Ireland. report-it.org.uk

National reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. actionfraud.police.uk

For Scotland, reports can be made to Police Scotland: scotland.police.uk/contact-us.

Get help and support

There are lots of organisations who work to support families and children. Visit childnet.com/get-help if you're worried about an online concern.

NSPCC 0808 800 5000
nspcc.org.uk
Free support and advice for adults concerned about the safety or wellbeing of a child.

family lives 0808 800 2222
familylives.org.uk
Free support and advice on any aspect of parenting and family life.

YOUNGMINDS 0808 802 5544
youngminds.org.uk
Fighting for young people's mental health
Free support and advice on how to support young people's mental health and wellbeing.

Helplines for children & young people

childline 0800 11 11
childline.org.uk
Providing help and support for under 18s.

THE MIX themix.org.uk
Providing help and support for 13-25 year olds.

@childnet

@childnetinternational



© 2024 Childnet International V09.24
www.childnet.com/education@childnet.com Registered UK Charity: 1080173

How Smoothwall protects against Ofsted's online safety guidelines

Oversee safe use of technology

With Smoothwall, you can rest assured that you are providing enterprise-level protection for your school, allowing your children to learn in a safe environment and use the internet as an aid to academic development.

Keep children and learners safe

Our real-time content aware web filter ensures that any unwanted content on the internet is kept out of reach for children. With the addition of our firewall, you can also ensure you are protected from external threats.

Flexible, age-appropriate e-Safety policy

Smoothwall allows you to easily build filtering policies based on the user or group. This means that administrators or delegated teaching staff can allow access for certain sites or apps for different groups of people.

Incidents are reported and monitored

Using our new safeguarding reports feature, you are able to monitor blocked actions and search terms, allowing you to identify any safeguarding concerns and report on it, keeping a full log of any incidents.

smoothwall
The Web You Want