

Online Safety Policy

Policy owner: Headteacher / Designated Safeguarding Lead

Approved by: Governing Body

Date approved: October 2026

Date of next review: October 2027

Review frequency: At least annually, and sooner where there are significant changes to legislation, guidance, technology, safeguarding risks or school practice

1. Introduction

Online safety is an important part of keeping children safe at Nun Monkton Foundation Primary School.

The internet and digital technologies are integral to children's education, communication, entertainment and everyday lives. They provide significant opportunities for learning and development but can also expose children to risks, including inappropriate or harmful content, harmful contact, online abuse, exploitation, bullying, misinformation, fraud and other forms of online harm.

The school has appropriate technical, organisational and educational measures in place to reduce these risks. However, no filtering or monitoring system can provide complete protection. Children therefore receive age-appropriate teaching about online safety and are encouraged to develop the knowledge, confidence and resilience to recognise and manage online risks.

Our aim is that all pupils will understand how to use digital technologies effectively, responsibly and safely, both in school and at home.

Online safety is a safeguarding responsibility shared by the whole school community.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Acceptable Use Policy/Agreement
- Data Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Remote Education arrangements, where applicable
- Complaints Policy
- Curriculum policies

- ICT/Technology and Cyber Security arrangements, where applicable.

This policy reflects the expectations of **Keeping Children Safe in Education 2026** and the Department for Education's **Filtering and Monitoring: Core Standard**.

2. Rationale

Digital technology is embedded in modern society and is an important part of education and children's lives.

Internet access is an essential educational resource and is used to support teaching, learning, communication, research and collaboration.

The school recognises that children may encounter online risks both inside and outside school. The school's responsibility is therefore not limited to preventing access to inappropriate material. We also teach pupils how to make safe and responsible choices, recognise potential risks, respond appropriately when something goes wrong and seek help from trusted adults.

Online safety education is therefore part of the wider safeguarding curriculum and is reinforced through Computing, Personal, Social, Health and Economic Education (PSHE), Relationships and Health Education, assemblies, pastoral support and other curriculum areas where appropriate.

3. Scope

This policy applies to all members of the school community who use or have access to school technology, systems or internet services, including:

- pupils
- teaching staff
- support staff
- supply staff
- governors
- volunteers
- trainee teachers
- contractors
- visitors
- parents/carers where relevant
- other users of school IT systems.

It applies to the use of school-owned or school-managed devices and systems both on and off the school premises, where applicable.

It also applies to personal devices when they are brought onto or used within the school environment or connected to school systems.

4. Roles and responsibilities

Online safety is everyone's responsibility.

4.1 Governing Body

The Governing Body has strategic oversight of online safety and should provide assurance that appropriate arrangements are in place to safeguard pupils and staff online.

The Governing Body will:

- ensure that online safety forms part of the school's safeguarding arrangements;
- ensure that appropriate filtering and monitoring systems are in place;
- receive appropriate assurance regarding the effectiveness of filtering and monitoring;
- ensure that the school's online safety arrangements are reviewed regularly;
- ensure that relevant policies are reviewed when legislation, guidance, technology or safeguarding risks change.

A governor with responsibility for filtering and monitoring will be identified.

Responsible governor:

Victoria Lindsay

4.2 Headteacher

The Headteacher has overall responsibility for implementation of this policy and will:

- ensure that appropriate online safety arrangements are in place;
- work with the DSL, Computing Lead and IT provider to manage online safety risks;
- ensure that staff receive appropriate information and training;
- ensure that safeguarding concerns are dealt with appropriately;
- ensure that filtering and monitoring concerns are acted upon;
- ensure that appropriate records are maintained.

4.3 Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding and child protection, including online safety concerns.

The DSL will:

- respond to safeguarding concerns arising from pupils' online activity;
- consider safeguarding alerts and reports arising from filtering and monitoring;
- ensure that online safety incidents are dealt with in accordance with safeguarding procedures;
- ensure that concerns and actions are appropriately recorded;
- liaise with external agencies where appropriate;
- work with IT support to understand filtering and monitoring risks;
- provide governors with appropriate assurance regarding filtering and monitoring;
- contribute to the annual review of filtering and monitoring provision.

DSL: Melissa Parker

Deputy DSL(s): Sarah Ritchie

All staff must report safeguarding concerns to the DSL or deputy without delay and follow the school's Safeguarding and Child Protection Policy. KCSIE 2026 emphasises that safeguarding concerns should be acted upon immediately and recorded with appropriate actions, decisions, rationale and outcomes.

4.4 Computing / Online Safety Lead

The Computing Lead will:

- support the development and delivery of the online safety curriculum;
- support staff in teaching safe and responsible use of technology;
- keep curriculum content under review;
- work with the DSL and Headteacher to identify emerging online safety issues;
- support pupils and staff in developing appropriate digital skills and resilience.

Computing / Online Safety Lead: Jessica Gill

4.5 IT provider / technical support

The school's IT provider or technical support will:

- maintain the school's filtering and monitoring systems;

- provide appropriate technical support;
- provide filtering and monitoring reports and alerts;
- investigate technical issues;
- complete agreed technical actions following incidents and system checks;
- support the school with annual filtering and monitoring reviews;
- advise the school when changes to technology or systems may affect safeguarding;
- ensure that filtering and monitoring remain appropriately configured following significant technical changes.

IT provider: NYES Digital

The DfE's current standard expects the DSL and IT support to work together, with clear responsibility for safeguarding and technical functions respectively.

4.6 All staff

All staff are responsible for:

- following this policy and the school's Acceptable Use Policy;
- supervising pupils appropriately when they use digital technology;
- modelling safe, respectful and responsible online behaviour;
- reporting online safety and safeguarding concerns promptly;
- reporting inappropriate or unexpectedly accessible online content;
- reporting suspected failures or weaknesses in filtering and monitoring;
- maintaining professional boundaries online;
- completing relevant training.

Staff must not assume that filtering and monitoring systems will prevent pupils from accessing inappropriate material.

5. Online safety curriculum

Online safety is taught explicitly and is also embedded throughout the curriculum and wider safeguarding programme.

Pupils will receive age-appropriate teaching about:

- online relationships and communication;
- privacy and personal information;

- passwords and account security;
- online identity and reputation;
- cyberbullying and harmful behaviour;
- inappropriate and harmful content;
- inappropriate contact and grooming;
- exploitation and online abuse;
- recognising manipulation and coercion;
- reporting concerns;
- misinformation and unreliable information;
- scams and fraud;
- safe and responsible use of the internet;
- digital wellbeing;
- appropriate use of images and video;
- copyright and intellectual property;
- safe and responsible use of social media and online communication;
- risks associated with sharing personal or sensitive information;
- the potential impact of online activity on mental health and wellbeing;
- appropriate use of artificial intelligence and AI-generated content, where relevant.

Pupils will be taught that they should tell a trusted adult if something online makes them feel worried, frightened, uncomfortable or unsafe.

Online safety education will be adapted according to pupils' age, maturity, additional needs and emerging risks.

6. Teaching children to respond to online risks

Children will be taught that they should:

- stop and think before communicating or sharing information online;
- protect passwords and personal information;
- question information rather than automatically believing it;
- avoid communicating with people they do not know where this may place them at risk;
- block or report inappropriate users where appropriate;
- tell a trusted adult about anything that causes concern;

- preserve evidence where appropriate and safe to do so;
- understand that they will not be blamed for reporting something that has made them uncomfortable or unsafe.

The school will maintain a child-centred approach to online safety and will consider the individual circumstances and needs of pupils when responding to incidents.

7. Filtering and monitoring

The school has appropriate filtering and monitoring arrangements in place to help protect pupils and staff from illegal, inappropriate and potentially harmful online content.

The school's current filtering provision is:

Filtering provider: Smoothwall

The school will ensure that filtering is appropriately configured for its pupils, staff and visitors and that the provision reflects the school's risk profile and educational requirements.

Filtering is preventative. Monitoring is reactive and may involve technical monitoring, manual monitoring or both.

No filtering or monitoring system can provide complete protection. Filtering and monitoring are therefore used alongside effective supervision, safeguarding procedures and online safety education.

The school will ensure that:

- school-managed devices are appropriately filtered and monitored;
- filtering is active and appropriately configured;
- safe search is enabled where appropriate;
- staff understand how to report inappropriate content or technical concerns;
- filtering does not unreasonably restrict legitimate teaching and learning;
- appropriate user profiles are applied;
- temporary exceptions to filtering are authorised and recorded where required;
- changes to devices, systems or services are checked to ensure filtering and monitoring remain effective.

The school will consider the filtering and monitoring implications of new technologies, including generative artificial intelligence.

The school will maintain appropriate arrangements with its IT provider to ensure that filtering and monitoring systems are maintained and updated.

8. Monitoring

Monitoring is used to identify activity that may indicate safeguarding, technical or inappropriate-use concerns.

The school's monitoring arrangements may include:

- in-person supervision of pupils using devices;
- technical monitoring of internet activity;
- network monitoring;
- device monitoring;
- alerts and reports generated by the school's monitoring system.

All staff should provide an appropriate level of in-person supervision when pupils are using devices.

The school's technical monitoring arrangements will provide:

- regular monitoring reports;
- immediate alerts for incidents categorised as high risk, where supported by the system;
- appropriate escalation of safeguarding concerns to the DSL;
- technical escalation to the IT provider where required.

The DSL will lead on safeguarding responses to monitoring alerts.

The IT provider will lead on technical investigation and remediation, working with the DSL and Headteacher where the issue has safeguarding implications.

The school will maintain records of significant monitoring incidents, including:

- the concern or incident identified;
- the date;
- the person who identified or received the alert;
- the action taken;
- any safeguarding referral or escalation;
- the outcome;
- any changes made to filtering, monitoring, supervision or practice.

All users of school systems will be informed that filtering and monitoring are in operation, in accordance with the school's privacy and data protection arrangements.

The DfE's current standard requires monitoring arrangements to include regular reports, immediate reporting of high-risk incidents and a documented record of actions and outcomes.

9. Annual review of filtering and monitoring

The school will review its filtering and monitoring provision **at least once every academic year** and sooner where required.

The review will involve, as appropriate:

- the Headteacher or nominated senior leader;
- the DSL;
- the IT provider/technical support;
- the responsible governor.

The annual review will consider:

- the school's pupil risk profile;
- age and maturity of pupils;
- SEND and other individual needs;
- use of technology in school;
- changes to devices or systems;
- filtering configuration;
- monitoring arrangements;
- monitoring incidents and safeguarding concerns;
- technical limitations;
- emerging online safety risks;
- use of generative AI;
- curriculum requirements;
- changes to relevant guidance;
- staff training;
- whether additional filtering or monitoring is required.

The outcome of the review will be recorded, including:

- the date of the review;
- who participated;
- what was reviewed;
- any identified weaknesses or risks;
- actions required;
- the person responsible for each action;
- timescales;
- completion of actions.

Filtering checks will also be carried out periodically according to the school's risk assessment and will be recorded.

The DfE's current standard requires an annual review and a record of checks including when they took place, who carried them out, what was checked and the resulting actions.

10. Responding to filtering and monitoring incidents

Staff must report immediately if:

- they access or witness inappropriate or harmful material;
- a pupil accesses inappropriate or harmful material;
- they believe filtering has failed;
- they identify a website or service that should reasonably be blocked;
- they identify unreasonable restrictions affecting teaching and learning;
- they suspect that a pupil or adult is deliberately attempting to bypass filtering;
- they suspect misuse of school technology;
- they identify a technical failure;
- they identify an online safeguarding concern.

Concerns should be reported to:

DSL: Melissa Parker

Headteacher: Melissa Parker

IT support: NYES Digital

Where a concern relates to safeguarding, the DSL will determine the appropriate response in accordance with the Safeguarding and Child Protection Policy.

Where a concern relates to technical filtering or monitoring, the IT provider will investigate and take appropriate action.

Where both safeguarding and technical issues are present, the DSL and IT provider will work together.

11. Reporting safeguarding concerns

All disclosures and concerns will be treated seriously and handled sensitively.

A child making a disclosure will be given an opportunity to explain what has happened in a safe environment.

Staff must:

- listen carefully;
- remain calm;
- avoid leading questions;
- not promise confidentiality;
- explain that information may need to be shared to keep the child safe;
- report the concern to the DSL or deputy without delay;
- record the concern accurately in accordance with school procedures.

Online safety concerns should be recorded on **MyConcern**, where this is the school's current safeguarding recording system.

The Safeguarding and Child Protection Policy will be followed for all safeguarding concerns.

KCSIE 2026 requires safeguarding records to include appropriate summaries, actions, decisions, rationale and outcomes.

12. Online abuse and harmful content

Online safety concerns may include, but are not limited to:

- cyberbullying;
- online harassment;
- grooming;
- sexual exploitation;
- sharing of intimate images;
- child sexual abuse material;
- exposure to pornography or other inappropriate sexual content;
- hate or discriminatory content;
- extremist or terrorist content;
- threats or intimidation;
- scams or fraud;
- harmful challenges;
- self-harm or suicide-related content;
- inappropriate contact;
- exploitation or coercion;

- deliberate attempts to bypass school filtering;
- illegal activity;
- inappropriate use of artificial intelligence;
- creation or distribution of harmful or deceptive AI-generated content.

Where an incident may constitute a criminal offence or place a child at risk of significant harm, the school will follow its safeguarding procedures and seek advice from the appropriate external agencies.

Staff must not investigate suspected criminal material themselves beyond what is necessary to establish immediate safeguarding information. They should follow the instructions of the DSL and relevant authorities.

13. Mobile phones and personal devices

Pupils are not normally permitted to use mobile phones or personal smart devices during the school day.

Where a pupil has an exceptional need to bring a mobile phone to school, prior permission must be obtained from the Headteacher.

Unless an alternative arrangement has been agreed, the device must:

- be switched off;
- be handed to the school office on arrival;
- be stored securely;
- be returned at the end of the school day.

The school reserves the right to respond to inappropriate use of personal devices in accordance with its Behaviour Policy, safeguarding procedures and Acceptable Use Policy.

Any safeguarding concern arising from a personal device will be dealt with under the school's safeguarding procedures.

14. Staff use of technology and social media

Staff are expected to maintain professional boundaries when using digital technology.

Staff must:

- use school-approved systems wherever possible;
- protect passwords and confidential information;
- avoid communicating with pupils through personal accounts;
- not share pupils' personal information or images through unauthorised services;
- maintain appropriate professional boundaries on social media;

- follow the school's Acceptable Use Policy and Staff Code of Conduct;
- report online safety or safeguarding concerns promptly.

Staff should not accept or initiate inappropriate online relationships with current pupils.

Any concerns about professional boundaries or inappropriate online behaviour will be dealt with in accordance with the school's safeguarding and staff conduct procedures.

15. Parents and carers

The school recognises that parents and carers play a vital role in keeping children safe online.

The school will support parents and carers by:

- providing online safety information;
- sharing appropriate guidance and resources;
- providing links to reputable organisations;
- including online safety information in newsletters and communications;
- raising awareness of emerging risks;
- encouraging parents/carers to discuss online experiences with their children.

The school may provide a regular online safety newsletter or online safety information through the school website and other appropriate communication channels.

Parents and carers are encouraged to contact the school if they are concerned about a child's online safety.

16. Online safety resources

The school may use resources from reputable organisations, including:

- Department for Education
- CEOP Education / Thinkuknow
- Childnet
- UK Safer Internet Centre
- Internet Watch Foundation
- BBC Bitesize
- Education for a Connected World
- other age-appropriate and professionally recognised resources.

Resources will be reviewed to ensure that they remain appropriate, accurate and relevant.

17. Artificial intelligence

The school recognises that generative artificial intelligence is increasingly accessible through websites, applications and digital devices.

The school will consider the safeguarding, educational, privacy and data protection implications of AI tools before they are introduced or used.

Where AI is used in school:

- pupils will receive age-appropriate guidance;
- personal or confidential information must not be entered into AI services unless the school has specifically authorised the service and appropriate data protection arrangements are in place;
- staff will follow the school's data protection and acceptable-use arrangements;
- AI-generated content will be treated critically and checked for accuracy;
- pupils will be taught, where appropriate, about misinformation, bias, manipulated content and other risks associated with AI;
- the school will consider whether its filtering and monitoring arrangements adequately address AI-generated and dynamically generated content.

The DfE's current filtering and monitoring standard specifically requires schools to consider the safeguarding implications of AI-generated content and to assess risks when introducing generative AI products.

18. Data protection and privacy

The school will comply with applicable data protection requirements.

Staff and pupils will be taught not to share personal or confidential information inappropriately.

The school will ensure that its filtering and monitoring arrangements are considered within its data protection arrangements.

Where appropriate, the school will maintain a Data Protection Impact Assessment (DPIA) for technical monitoring systems and review privacy information relating to third-party providers.

Monitoring and filtering will be undertaken proportionately and for legitimate safeguarding, educational and operational purposes.

19. Cyber security

The school recognises that cyber security is an important part of online safeguarding.

The school will maintain appropriate arrangements to reduce the risk of:

- unauthorised access;
- loss of data;
- malware;
- phishing;
- compromised accounts;
- inappropriate sharing of passwords;
- unauthorised software;
- cyber attacks.

Staff and pupils will be taught appropriate cyber security practices, including the importance of strong passwords, protecting login information and reporting suspicious activity.

20. Remote and off-site use

Where school-managed devices or accounts are used outside school, the same safeguarding and acceptable-use expectations apply.

The school will ensure, where technically applicable, that filtering and monitoring arrangements continue to protect school-managed devices when they are used away from school.

Staff and pupils should report online safety concerns arising from remote or off-site use in accordance with this policy.

21. Visitors and volunteers

Visitors, volunteers and other adults who use school IT equipment or systems will be made aware of the school's relevant acceptable-use and safeguarding expectations.

Where appropriate, visitors or volunteers will be required to comply with the school's Acceptable Use Policy.

Visitors must not use school technology to access inappropriate content or communicate with pupils through unauthorised channels.

22. Training

The school will provide staff with appropriate information and training to enable them to:

- understand current online safety risks;
- use technology safely;
- recognise online safeguarding concerns;

- understand filtering and monitoring arrangements;
- report filtering and monitoring concerns;
- respond appropriately to disclosures;
- understand their professional responsibilities;
- recognise emerging risks, including those associated with AI.

Training will be refreshed as necessary and in response to changes in guidance, technology or identified safeguarding risks.

23. Review and evaluation

This policy will be reviewed at least annually and sooner if required.

The review will consider:

- changes to legislation and statutory guidance;
- KCSIE;
- DfE filtering and monitoring standards;
- safeguarding incidents;
- filtering and monitoring reports;
- technical changes;
- emerging online risks;
- changes to pupil needs;
- staff feedback;
- parental feedback where appropriate;
- curriculum developments;
- introduction of new technologies, including AI.

The effectiveness of this policy will be evaluated through safeguarding records, filtering and monitoring reviews, staff feedback, pupil feedback, governor oversight and other appropriate evidence.

24. Related policies and documents

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Acceptable Use Policy

- Data Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Complaints Policy
- Cyber Security arrangements
- Privacy Notices
- Remote Education arrangements, where applicable
- Filtering and Monitoring Review Record
- Filtering and Monitoring Incident Log

25. School aims

This policy supports the school's aims to:

Appendix 1 – Online Safety: pupil expectations

Pupils are expected to:

1. Use school technology responsibly.
2. Keep passwords and personal information private.
3. Treat other people respectfully online.
4. Tell an adult if something online makes them worried, frightened or uncomfortable.
5. Not deliberately access inappropriate or harmful material.
6. Not attempt to bypass school filtering or security.
7. Not take, share or publish photographs, videos or recordings of others without appropriate permission.
8. Not communicate with others online in a way that could be harmful, threatening or inappropriate.
9. Check information before believing or sharing it.
10. Follow staff instructions when using digital technology.

Appendix 2 – Online Safety: staff response to an incident

Where a member of staff becomes aware of an online safety concern:

1. Stop / secure the immediate situation

Where appropriate, stop the activity and ensure that the pupil is safe.

2. Do not investigate unnecessarily

Do not search through devices, accounts or messages beyond what is necessary to establish immediate safeguarding information.

3. Report

Inform the DSL/deputy without delay where the concern has safeguarding implications.

4. Record

Record the concern and actions taken using the school's safeguarding recording system where appropriate.

5. Technical response

Report technical issues, filtering failures or suspected attempts to bypass controls to the IT provider in accordance with school procedures.

6. Follow-up

The DSL and/or Headteacher will determine whether further safeguarding action, parental contact, external referral, technical action, curriculum intervention or other response is required.

Appendix 3 – Filtering and monitoring annual review

The school will maintain a separate record of its annual filtering and monitoring review.

The record should include:

- date of review;
- names/roles of those involved;
- filtering provider;
- monitoring provider/system;
- devices and services considered;
- user groups considered;
- filtering configuration;
- monitoring configuration;
- checks undertaken;
- incidents and alerts reviewed;
- technical limitations identified;
- safeguarding risks identified;

- AI and emerging technology considerations;
- staff training considerations;
- actions required;
- person responsible;
- deadline;
- date action completed.

Filtering and monitoring checks should also be recorded periodically throughout the year according to the school's risk assessment.

Policy review date: September 2026

Next review: October 2027

Approved by Governing Body: October 2026



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



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.



WWW.CHILDNET.COM

Programme and UK Childnet (188 072)

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

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 0800 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.

YOUNG MINDS 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.

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

@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