THE SNAITH SCHOOL

Online Safety Policy

Version 1.1

Name and Title of the Author:	Richard Wilson Assistant Headteacher
Name of Responsible Committee / Individual:	Local Governing Body
Implementation Date:	Spring 2022
Review Date:	September 2025
Next Review	September 2027
Related Documents:	Child Protection and Safeguarding Policy 2025 Mobile Phone Policy ICT Acceptable Use Policy Anti-Bullying Policy

CONTENTS

SECTION **PAGE**

Introduction

Technology plays a vital role in safeguarding young people, offering valuable opportunities for learning and development. However, it also presents risks that can facilitate harm. Recognising this, Keeping Children Safe in Education identifies four key categories of online safety risk:

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – Exposure to illegal, inappropriate, or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact** – Harmful interactions with others online, including peer pressure, commercial advertising, and adults posing as children or young adults with the intent to groom or exploit for sexual, criminal, financial, or other purposes.
- **Conduct** – Personal online behaviours that increase the risk of harm, such as the creation or sharing of explicit content (e.g., consensual and non-consensual nudes or pornography), and online bullying.
- **Commerce** – Exposure to risks such as online gambling, inappropriate advertising, phishing scams, and financial fraud.

This policy has been developed with those categories in mind and outlines the roles, responsibilities, and procedures necessary to promote and maintain online safety across our school community.

Aims

This policy sets out the school's approach to creating a safe digital environment for all members of the school community, both on and off the school premises. It outlines how the school will:

This policy sets out the school’s commitment to:

- Providing a safe and secure digital environment for all members of the school community.
- Promoting safe, responsible, and appropriate use of technology.
- Ensuring that staff and pupils understand their responsibilities in using ICT both within school and in their personal lives;
- Responding effectively to any incidents or concerns related to online safety.

It also clarifies the responsibilities of key individuals in implementing and maintaining a whole-school approach to online safety.

This policy applies to all members of the school community, including staff, pupils, parents, and governors. It should be read in conjunction with relevant supporting policies and guidance documents listed below.

We believe that ICT is a powerful tool that can enrich teaching and learning across the curriculum. It enhances the educational experience of pupils and provides staff with resources to support effective teaching.

While the benefits of technology are significant, we are also aware of the potential risks posed by the internet and other digital platforms. As such, we consider online safety to be a collective responsibility, requiring the active participation of the entire school community.

Social networking platforms and digital tools are increasingly used to support learning, promote creativity, and share content. We encourage staff to make appropriate and innovative use of these technologies to enhance their educational experience.

However, all use must be conducted in a safe and responsible manner. Staff are expected to maintain a professional standard of conduct in their use of social media and other online platforms, modelling appropriate behaviour for pupils and upholding the values of the school.

Risks and Responsibilities

Risks of ICT use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of the internet and ICT.
- Exposure to age-inappropriate materials.
- Inappropriate or illegal behaviour.
- Physical danger or sexual abuse.
- Being subjected to harmful online interaction with other users.
- Inappropriate or illegal behaviour by school staff.
- Actions that bring the school into disrepute.
- Online grooming or child exploitation.

[1] This list is by no means exhaustive, but means to highlight some of the main areas of risk that the school has identified.

Creating a Safe ICT Learning Environment

The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of **whole-school awareness, designated responsibilities, policies and procedures**. This is achieved by:

   - Raising awareness of the risks of ever-changing technology that is both emerging and already embedded in the school community.
   - Ensuring that the Online Safety policy and education programme adapts to meet these new and emerging technologies and is reviewed as incidents occur.
   - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to online safety.
   - Ensuring that the school's policies and procedures are effective and kept up to date, and also make clear to all members of the school community what is acceptable when using ICT and the internet.

2. Make use of effective technological tools to ensure the safe use of the internet and school ICT systems. These include:

   - Firewall protection to the school's network.
   - Virus protection of all relevant IT equipment connected to the school's network.
   - Filtering, logging and content control of the school's internet connection.
   - Monitoring systems.

3. Develop an Online Safety education programme for the whole school. This will consist of:

   - An on-going education program for the pupils at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
   - Continued professional development for staff to ensure that they are equipped to support the pupils at the school and are also fully aware of their responsibilities in using ICT, both in and out of the school.
   - An on-going education program for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the school in these matters.
   - Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
   - Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
   - Explaining how accessing and/or sharing other people's personal information or photographs might be inappropriate or illegal.
   - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
   - Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.

Headteacher's Responsibilities

1. To take ultimate responsibility for online safety whilst delegating the day-to-day responsibility to the Online Safeguarding link (OSL).
2. To ensure that the OSL and the members of the online safety teams are given enough time, support and authority to carry out their remit.
3. To ensure that the governing body is kept informed of the issues and policies.

4. To ensure that appropriate funding is available to support the technological infrastructure and CPD training for the online safety programme.

Governing Body's Responsibilities

1. To ensure the designated Safeguarding Governor considers online safety as a part of the regular review of child protection and safeguarding.
2. To support the Headteacher and OSC to ensure that the correct policies and procedures are in place, and also that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of online safety to parents.

Online Safeguarding Link Responsibilities

1. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of online safety inside and outside of the school environment.
2. To work with the appropriate members of staff to develop an online safety education program for the pupils.
3. To maintain a log of all online safety incidents that occur in the school.
4. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
5. To meet with the Designated Safeguarding Lead (DSL) regularly to discuss online safety and progress.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
7. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the OSC, Headteacher and Police if necessary.
8. Review the technological systems upon any discovery or breach of the Acceptable Use Policy (AUP), so that where possible a breach can be prevented from reoccurring.
9. Liaise with the pastoral team if any breach can be traced back to an individual pupil.
10. Liaise with the DSL and Headteacher if any breach can be traced back to an individual member of staff.
11. Provide the technological infrastructure to support the online safety policies and procedures.
12. Report any network breaches of the school's Acceptable Use Policy or online safety Policy to the OSC.
13. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Designated Safeguarding Lead's Responsibilities

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
2. To develop and review the appropriate online safety policies and procedures.
3. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
4. To work with the appropriate members of staff to develop a parental awareness programme for online safety at home.
5. To liaise with the OSL on specific incidents of misuse.
6. To liaise with any outside agencies as appropriate.
7. Take a proactive role in the online safety education of the school's pupils.
8. Develop systems and procedures for supporting and referring pupils identified as victims or perpetrators of online safety incidents.
9. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Subject Leaders' Responsibilities

1. To work with the OSL to develop an area/departmental policy to ensure that online safety is embedded in their areas teaching practice, where appropriate.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
3. To alert the OSL to the creation of any school social media accounts.

Pastoral Staff Responsibilities

1. To act as a key member, and first point of contact for the school's online safety team.
2. To support the OSL in the development and maintenance of appropriate policies and procedures relating to pupil welfare.
3. To develop and maintain their own knowledge of online safety issues.
4. To ensure that any incidents of ICT misuse are dealt with through the correct channels, in line with the ICT Acceptable Use Policy, Behaviour Policy and Online Safety Policy.
5. To ensure that any pupils who experience problems when using the internet are appropriately supported, working with the OSL and Safeguarding Officer (SO) as required.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Special Educational Needs Coordinator's Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard as to how they may affect children and young people with additional educational needs.
2. To develop and maintain additional policies and online safety materials in conjunction with the OSC, tailored to meet the needs of SEN pupils.
3. To liaise with parents and carers of SEN pupils to raise awareness of the school's online safety position and how the parents can support the school's position.
4. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Classroom Teachers, Teaching Assistants, Pastoral Staff and Cover Supervisors' Responsibilities

1. To develop and maintain a knowledge of online safety issues, with particular regard to how they might affect children and young people.
2. To implement school and departmental online safety policies through effective classroom practice.
3. To ensure any incidents of ICT misuse are reported through the correct channels.
4. To ensure that the necessary support is provided to pupils who experience problems when using the internet, and that issues are correctly reported to the OSC and the pastoral team.
5. To plan classroom use of ICT facilities so that online safety is not compromised.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
7. To alert the OSC to the creation of any school social media accounts.

Pupils' Responsibilities

1. To uphold all school online safety and ICT policies.
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they, or another pupil experience problems online.
4. To communicate with their parents or carers about online safety issues and to uphold any rules regarding online safety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting online safety.
2. To discuss online safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the school.

Procedures and Implementation

The school, through the Online Safeguarding Link, will ensure that all staff are aware of the policies and procedures being implemented to meet the Online Safety requirements. There will be information available to all staff about the technologies that are already in use at school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback on the school's online safety discussions, be given clear guidance with what the procedures are and know who they should speak to regarding any issues.

In the first instance, all staff will receive a basic introduction to the online safety programme at the school,and be directed towards the resources that have been made available.

The OSL will work with the HR Team and senior leader responsible for CPD to ensure that the school's induction and CPD programmes include adequate provision for the delivery of online safety training.

Online safety will form a part of the Safeguarding Induction for new staff starters and direct them towards the existing policies, procedures, resources and courses of action.

Pupils

The pupils at the school will be made aware that there is a whole school approach to online safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Pupil members will be invited to participate in future planning and discussions regarding online-safety and their opinions will be regularly gauged as to the effectiveness of the provision.

Through assemblies, pupils will be made aware of policies and methods of enforcing these policies.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that The Snaith School is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

Parental workshops will be offered to give parents the opportunity to understand online safety topics and new risks children are opposed to.

Technical – infrastructure/equipment, filtering, and monitoring

Firewall

- The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analyzed for security audits.

- The responsibility lies with the IT site lead and TEAL engineer for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Anti-Virus Protection

- The school has purchased a third-party security suite from Heimdal Security, which compromises a number of security tools to protect our network including; anti-virus, auto patching applications and malware redirect detection.

- It is the responsibility of the OSL to ensure that all necessary computers on the school network are running current anti-virus software and that regular scans are performed. If a virus out-break happens, the Network Manager must notify the SLT link for IT and/or Headteacher and as soon as possible isolate the infection.

- Personal devices for staff should connect to the Snaith "devices" network using their computer credentials to authenticate, this wireless network is ring-fenced by a firewall to protect internal network devices and only allow certain internal applications to connect. Visitors must obtain a key from the IT Support team or reception and use the Snaith "TSSGuest" wireless network, which is a less filtered connection to provide guests an internet connection, secure sites are also not logged on this wireless network. Any devices being brought into to school and connected to the school's ICT network via Ethernet to obtain a wired connection to the network must be proven to have up-to-date Anti-Virus protection and be cleared by the Network Manager before being connected.

- Pupil Devices which are provided and used by pupils at home are also covered by the filtering and monitoring systems as if they were in school.

- Whilst the Heimdal antivirus and filtering system in place will attempt to eliminate all potential threats, it is the responsibility of the end user to ensure that they do not open emails, including attachments, from any third party whom they do not know. Any such emails and/or attachments should be reported to the IT support team.

Filtering and Logging of Internet Access

- The school has a web caching and proxy server (Smoothwall) that contains accredited filter lists. This enables the school to log all Internet traffic in the school and allow different sites to different groups of users. This server ensures that all internet use on the school's network is logged to an individual user of the network. If the device being used to access the Internet is not a school owned device, the user will have to present valid school network credentials before they can gain any access to the school's Internet connection. If an online safety incident requires it, all Internet access logs of any pupil or staff member can be retrieved to support any required processes.

- It is the responsibility of the OSL to ensure that all computers connected to the school's network only receive an Internet connection by going through the proxy server. The IT site lead, on request of the OSC, will add any sites that have been discovered through online safety incidents to the block lists of the filtering server. The IT site lead will perform regular reports from the logs of the web proxy server to present to the OSC and SLT link for IT, with regards to the most accessed sites and most active Internet users in the school.

Monitoring systems

The school has many different monitoring systems at its disposal.

- All files stored on the school's servers can be searched and checked.
- Teachers can monitor the pupils use of computers within the IT rooms they are in
- All computer use is monitored centrally against a set of predefined word lists and use or viewing of inappropriate text is logged with a screen grab and the details of the offence, user, and time it occurred.
- Any incident that has a sanction attached to it is entered into the school's MIS system.
- Computer use is live monitored using Smoothwall Monitor Managed Service with incidents alerted to the OSC, CPO and Network Manager.

The Network Team will perform a scan of all staff and pupil home drives for all images and identify any inappropriate images saved. This will be performed once every term and any inappropriate images found, the OSL will notify the DSL providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

Senso and Smoothwall Monitor will flag identification of any keywords identified from a pre-populated list. The Smoothwall monitor will raise an alert, based on the context. OSL, SO and DSL will access and review these logs of and respond accordingly to any breaches of the AUP or other online Safety incidents recorded.

Any incident that has a sanction attached will be recorded in the SIMS system using the behaviour type of **ICT AUP Breach**. These incidents can then be reported upon and shared with relevant Head of House and Subject Leaders as required.

Where incidents raise concern regarding a child’s welfare they will be also recorded on our online Child Protection Monitoring System CPOMS where a pattern of concern can be identified if appropriate.

<u>Training</u>

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required through our regular safeguarding bulletin.

Training in the use of the IT monitoring software will be offered to all staff. The procedure for reporting online safety incidents will detail the information needed from staff when reporting an incident recorded by this software.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse

- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy and our "Staff Engagement Plan" Appendix 4

Online Safety Education

All pupils at the school will receive an on-going online safety education programme.

This programme will inform the pupils of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The ICT & Computing department run a distinct six-week e-Safety unit with every Year 7 pupil through their weekly ICT lessons. The content of these lessons is regularly reviewed to include up to date issues. Currently the unit is developed in line with DfE guidance and covers:

Content Risks:

- Identifying fake content.
- Risks associated with social media (violence, hate speech, pornography, etc.)

Contact Risks:

- Grooming.
- Image sharing.
- Scams.

Conduct Risks:

- Web archiving & Digital footprints.
- Bullying.
- Obsession & Self Image.

Commerce:

- Online gambling
- Inappropriate advertising
- Phishing scams
- Financial fraud.

The School's PSHE curriculum is under constant review to include emerging trends in pupils' online use and to address new uses as they arise. Currently this covers:

Year 7 (Spring 1) - How can I stay safe online and in person?

- Sharing private and personal life online and offline, social media, cyberbullying, online challenges, trolling, online scams.

Year 8 (Autumn 2) - What is attraction?

- The law on pornography

Year 8 (Spring 1) - What are the dangers of online and personal safety?

- Gambling and child sexual exploitation

Year 9 (Autumn 2) - What are safe relationships? Online or in person

- Sexting and digital footprints

Year 9 (Spring 1) - How do I manage a dangerous situation?

- Extremism and child sexual exploitation/grooming

Year 10 – What is acceptable and unacceptable in a relationship?

- Stalking and harassment
- Sexting, pornography and revenge pornography

Year 10 – Is our world fair?

- Social media validation and safety

Year 11 - How do I take care of my own health and well-being?

- Gambling and addiction Body image

The school will follow the Safer Internet Day programme and deliver those resources through assemblies. Form tutors will be informed about the content being delivered, and asked to discuss the content after the assembly is given so that pupils have an opportunity to raise any concerns or issues from this information.

The APEX curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.

The SENCO will work with the OSL to ensure that there are accessible and adequate resources available for SEND pupils of the school to access the same online safety education as the rest of the school.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT.

The Snaith School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

TSS will treat any use of AI to bully pupils in line with our Anti-Bullying policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by TSS

Responding to a concern

Appendix 1 outlines the process regarding concerns being raised relating to online safety. In the first instance any concern should be reported to the pupil's year leader.

As a school, we proactively work to ensure the safety of our pupils both in-school and online. We do not have the capacity to police all online activity outside of school, however where actions of a pupil online go against our code of conduct, as outlined in the School's Behaviour Policy, we will sanction pupils, following the expectations set out in our Behaviour for Learning Policy.

Where actions taken by pupils online pose a risk to them or others, they will be dealt with in line with our Child Protection Procedure, conducting appropriate risk assessments and ensuring minimal disruption to any victim, where appropriate.

Consistent Approach

The DSL will work with the pastoral team to ensure there is a commonality of approach in responding to online safety incidents and that the correct reaction and procedure is followed by all staff when dealing with an online safety issue.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. For Pupils this will be in accordance with the Discipline and Rewards Policy. Staff incidents will be dealt with under the Staff Code of Conduct and Discipline Policy and Procedures.

Examples of pupil incidents are outlined in the table below, along with a possible response. However, each incident will be reviewed on a case-by-case basis and the sanction will be dependent on the seriousness of the offence.

Examples of Pupil Incidents	Issue a Warning	Issue a behaviour detention LD or ASD	Restriction of technology and network/internet access rights	Further sanction e.g. RESET, Internal Suspension & Suspension
Unauthorised use of non-educational sites during lessons	X			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X		
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X		
Unauthorised downloading or uploading of files		X	X	
Deliberately accessing or trying to access material that could be considered illegal.				X
Deliberately manipulating media to misrepresent a person or their actions				X
Allowing others to access School network by sharing username and passwords			X	X
Attempting to access or accessing the School network, using another Pupil's account		X	X	X
Attempting to access or accessing the School network, using the account of a member of staff			X	X
Corrupting or destroying the data of other users		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			X	X
Using proxy sites or other means to subvert the School's filtering system			X	X

Deliberately accessing or trying to access offensive or pornographic material			X	X

School Social Media Accounts

The school will support departments wishing to set up social media accounts. Whilst all social media is different, and constantly evolving there are some key expectations for colleagues using social media in school, which are as follows:

Any colleague wishing to set up a school or departmental social media account should first seek approval from their line manager and then the OSC.
All social media must be set up to ensure that that there can be no private communication or Direct Messaging between the account and the accounts of pupils.
A log of all social media accounts in school should be kept by the OSC.
Passwords should not be shared between colleagues and one colleague should take overall responsibility for the account and its content.
Users should follow the expectations and responsibilities of colleagues outlined above.

As stated above, social media is constantly changing and as such advice should be sought from the OCS and Network Manager where appropriate.

Legislation, guidance, Links to other organisations and documents

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

The following links provide additional advice or guidance with regard to online safety:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Netsmartz - http://www.netsmartz.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance –

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_H eadteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – oung peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides) DfE
advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released) ICO
Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support NCA
– Guide to the Computer Misuse Act NEN –
Advice and Guidance Notes

Working with parents and guardians

Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers Get
Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

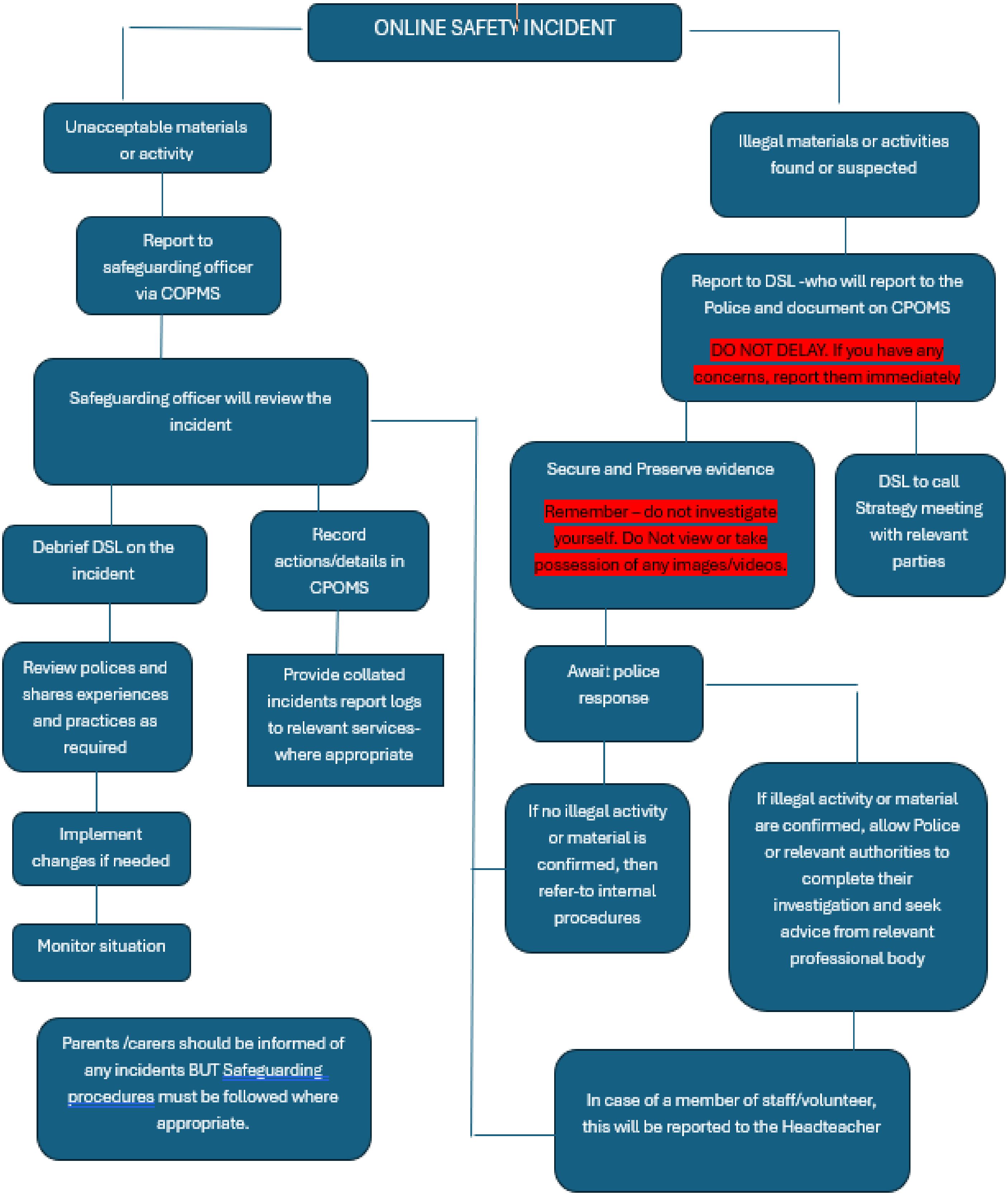
Prevent Duty Guidance
Prevent for schools – teaching resources NCA
– Cyber Prevent
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Appendix 1- Responding to incidents of misuse



ONLINE SAFETY INCIDENT

Unacceptable materials or activity

Report to safeguarding officer via COPMS

Safeguarding officer will review the incident

Debrief DSL on the incident

Review polices and shares experiences and practices as required

Implement changes if needed

Monitor situation

Record actions/details in CPOMS

Provide collated incidents report logs to relevant services- where appropriate

Parents /carers should be informed of any incidents BUT Safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to DSL -who will report to the Police and document on CPOMS

DO NOT DELAY. If you have any concerns, report them immediately

Secure and Preserve evidence

Remember – do not investigate yourself. Do Not view or take possession of any images/videos.

DSL to call Strategy meeting with relevant parties

Await police response

If no illegal activity or material is confirmed, then refer-to internal procedures

If illegal activity or material are confirmed, allow Police or relevant authorities to complete their investigation and seek advice from relevant professional body

In case of a member of staff/volunteer, this will be reported to the Headteacher

Appendix 2 – Acceptable Use of ICT Policy for Staff

THE SNAITH SCHOOL

STAFF POLICIES AND GUIDANCE THAT YOU MUST READ AND AGREE TO ACCEPT

Staff agreement to work according to the Safeguarding policies of the Education Alliance and The Snaith School. These policies and guidance include: -

- Child Protection
- Criminal Record Checks Policy and Procedure
- Keeping Children Safe in Education
- Safer Working Practices with Children and Young People
- Safe School, Safe Children, Safe Staff Code of Conduct
- Physical Intervention and Restraint
- Whistleblowing
- Social Media Guidelines
- ICT Acceptable Use Policy
- E-safety (The school has provided computers for use by staff, offering access to vast amounts of information for use in studies, offering enormous potential to support the curriculum) - please see key points for staff below:

ICT ACCEPTABLE USERS POLICY (AUP) KEY POINTS FOR STAFF:

Equipment

- Should you require any software and/or hardware installed on the school network always get permission and/or seek advice from the IT team.
- Damaging, disabling, or wasting resources (personal printing) is not acceptable.
- Only use school computers for educational interest purposes, personal interests should be kept to personal break times and is always monitored. Buying or selling goods is inappropriate.
- Personal Devices may be connected to the school wireless network, the AUP will apply to the use of these devices and internet activity will be filtered and logged.
- Do not let family members use the school IT equipment (laptop, iPad, cameras etc.) these are supplied for use by staff only.
- You also have the ability to install your own software and apps. It is your responsibility to ensure that any software that you install is legal (personal data is your responsibility; if your laptop is repaired or replaced we will not copy across music, photos etc. that are not for teaching purposes).
- Protect Devices from spillages by eating or drinking well away from IT equipment.
- iPads are provided to staff as a teaching & learning tool, pupils should not be allowed to use them, they are a personal device and should only be used with your own Apple ID.
- The management of data both school & personal on the device is your own responsibility and you are responsible for backing up the content of your iPad to the apple ID that is used on the device
- Photographs and videos of staff and pupils must not be uploaded onto any public websites.
- The Snaith School will install a Mobile Device Manager to allow the installation of Apps and to enable resets and recovery, this profile should not be removed from the device.
- iPads supplied to staff are provided with a good quality case, the iPad should not be removed from the case supplied and any damage occurring when the case is removed will be charged to the member of staff.
- iPads are not covered by the school insurance policy and should be kept securely off-site and protected with the lock code. Individual staff will be expected to take responsibility for the device outside of school, therefore careful consideration must be given to where it is used. Staff may wish to take out personal insurance for the device if taking on holiday etc.
- Every care should be taken to ensure the iPad is not damaged. Any damage should be reported immediately to ICT Support. On completion of the iPad repair form each individual case will be considered. Contribution to the repair costs may be required
- Portable devices must be stored in a secure environment.

- When in public places (even your office, if it is not locked) users must ensure portable devices remain in the close proximity and are never left unattended.
- Staff must avoid unauthorised viewing of sensitive or confidential data in public, home or common areas.
- Staff must not leave portable computing devices (laptops, iPads) in an unattended vehicle (unless absolutely unavoidable) and if you have to, it should be locked in the boot.

Security and Privacy

Ensure that you use a suitably complex password for access to the Internet and ICT systems. Please note the following:

- Keep passwords secure from pupils, family members and other staff.
- Use a different password for accessing school systems to that used for personal (non-school) purposes.
- Do not allow passwords to be remembered automatically within the machine internet browser or any other remote access.
- **Do not leave unattended computers logged on either lock the machine, log out or lock the room.**
- **Do not disable the passcode on your school iPad.**
- Never use someone else's logon name or password.
- Proceed with caution when asked to disclose any personal details. (address, telephone number, pictures etc) Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- Respect the security of the network.
- School computers are shared resources. There is a risk that private/confidential information could fall into the wrong hands! (Bank, Credit card details and other personal information).
- Internet access is filtered for the benefit of all users. Any anomaly of sites that are filtered or not should be reported to the ICT support team.
- **In order to safeguard you and others**, the school reserves the right to monitor **communications**, examine or delete any files that may be held on its computer systems.
- **You have personal responsibilities in relation to GDPR and the privacy and disclosure of personal and sensitive confidential information.**

Internet

- Access of the Internet should be for school purposes.
- Limited personal use of the internet is permitted in your own time only (i.e. during lunch breaks, prior to the start of the working day, at the end of the working day and for teaching staff during break times and free periods). This use must be in line with the guidance in this policy.
- Only access suitable material; using the Internet to obtain, download, send, print, display, transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people both outside and inside the school. This includes abiding by copyright laws.

Email

- Be polite and appreciate that other users might have different views from your own.
- Only open attachments to emails if they come from someone you already know and trust.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, report such messages to a member of ICT support team and **or e-safety coordinator**
- **When communicating on behalf of school <u>only</u> use your school email address for all correspondence with staff, parents or other agencies.**

Mobile phones and Devices

- Staff should not contact parents or pupils on personally owned devices, if absolutely necessary you must hide your number by inserting 141 before dialling the number.
- Do not use personally owned mobile devices to take images or sound recording.

- Social
  Media
- You should set and maintain a profile on social networking sites to maximum privacy and give access to known friends only.
- Do not use social media tools to communicate with current pupils.
- If you experience derogatory or slanderous comments relating to you, the school, or colleagues, take screenshots for evidence and report to the school e-safety coordinator. Do not respond to these communications directly.

Criminal Records Checks

The school carries out an Enhanced with Barred List check on each new member of staff. If you are convicted of a criminal offence or receive a caution, reprimand, or warning at any time during your employment at the school, it is essential that you inform the school's Executive Principal (Scott Ratheram), Trust Safeguarding Lead (Debbie Dalton) or HR Manager (Sue Lord) immediately. This is in line with the trust's DBS policy. Failure to disclose any criminal activities or investigations, convictions or warnings may result in an investigation under the trust's Disciplinary Policy and Procedure.

AGREEMENT

I have read and understood all the above in relation to The Snaith School safeguarding policies (including the school's Acceptable Users Policy) and that failure to abide by these policies and guidance may result in disciplinary action.

IF YOU DO NOT ACCEPT, you will be logged out of the system and will be denied access to all of our resources.

Appendix 3 – Acceptable Use of ICT Policy for Pupils

THE SNAITH SCHOOL ACCEPTABLE USE OF ICT POLICY PLEASE READ

CAREFULLY

You must agree to follow these simple rules in order to access the school's ICT facilities.
ICT equipment is provided for the benefit of all pupils and staff. Please be responsible at all times.

I WILL:

Equipment

Treat all ICT equipment with care

Only use school ICT equipment for educational purposes

Think before I print

Not eat or drink in ICT rooms

Security and Privacy

Not attempt to bypass security systems

Ensure that my password to access the ICT system is difficult to guess and I will not share it with others

Internet

Not search for, download, upload or forward any content that is illegal

Only access the internet for educational purposes

Not access social networking sites through the school network

Social media

Obey age restrictions placed on social networking sites

Set my account settings to private

Not abuse any members of staff or pupils when publishing online

Not make comments about the school which could damage its reputation

Mobile phones and devices

Ensure that my mobile phone and any other device is switched off/muted inside school buildings and in my bag

Not use any personally owned device to take images, video or sound recordings without permission

Accept that my mobile phone may be confiscated if I break these rules

E-mail

Use my school email address to communicate on school matters

Only open e-mails if I can trust the sender

Report any e-mails that contain inappropriate images or words (swearing or offensive language) to my teacher

I UNDERSTAND:

All use of computer activity is recorded and can be used for evidence if required

That my account is my responsibility and allowing others to use the account is prohibited

Failing to follow this policy will result in a temporary or permanent ban from the school's IT system

Agreement

I have read and understood all of the above listed points and know that failure to follow these rules will lead to access being denied to the school ICT network. Further action may be taken in line with The Snaith School Acceptable Users Policy (AUP).

If you do not ACCEPT this policy you will be logged out of the system. You should talk to your teacher and explain why you will not agree to the conditions.

Digital Safety Parental Engagement

Online Safety Hub

The Education Alliance Trust

2025 / 2026

Introduction

This document provides you with all the information you need to easily maintain an annual Parental Engagement Programme. The purpose of the plan is to educate and support your parents in navigating their children's digital safety and well-being and encourage uptake of both the Online Safety Hub and the Qustodio online safety parent app.

We suggest sending out the follow-up communications to parents, in order to help promote and encourage up-take of both the Online Safety Hub and the Qustodio app.

The communications include an email, social media posts and text messages to parents.

Additionally, we recommend sharing Online Safety Hub articles with parents throughout the school year, across all relevant communication channels. These channels may include for example, weekly emails, newsletters, social media pages, or text messages.

To help you drive engagement with parents, please see below ready-to-go written material for these communications.

1. Email to Parents - 12/9/25

Dear Parent,

Find out how to keep your child safe online.

Don’t forget that the Online Safety Hub is now live! You can access it for free here:

https://theeducationalliance.onlinesafetyhub.uk/

The Online Safety Hub is a brand-new online resource with lots of expert advice and guidance to help you manage your child's safety online as a parent.

It includes information on the latest hot topics when it comes to keeping children safe, such as how to manage your child's screen time, understand the latest gaming platforms, what they mean for your child’s safety and lots more.

We’re also offering you as a parent, a free Qustodio account facilitating parental controls on any individual device and free premium access for 30 days. Gain more visibility on what’s going on in your child’s online world. Block dangerous content, introduce screen-free schedules, receive alerts for inappropriate content, keep tabs on their location and more. Follow the link to create your free account

https://www.qustodio.com/en/30-days-school-special/?utm_source=internal&utm_medium=OSHub&utm_campaign=theeducationalliance

If you have any questions on any of the above, please get in touch.

2. Social Media Posts – HYA 15/9/25

- Social Media Post 1 - Online Safety Hub

You can now access the Online Safety Hub FOR FREE. Head to the Online Safety Hub for lots of expert advice and guidance to help you manage your child's safety online. It includes information on the latest hot topics when it comes to keeping your child safe, such as how to manage your child's screen time, understanding the latest gaming platforms, what they mean for your child's safety and lots more. Simply follow the link to access The Online Safety Hub:

https://theeducationalliance.onlinesafetyhub.uk/

- Social Media Post 2 - Qustodio Online Safety Parent App HYA 16/9/25

Don't forget to sign up for your FREE Qustodio. Gain more visibility on what's going on in your child's online world and make sure they are kept safe. Block dangerous content, introduce screen-free schedules, receive alerts for inappropriate content and more.

Follow the link to create your free account:

https://www.qustodio.com/en/30-days-school-special/?utm_source=internal&utm_medium=OSHub&utm_campaign=theeducationalliance

---

3. Text Messages

- Text Message 1 - Online Safety Hub

Parent, you can now access the Online Safety Hub FOR FREE. It helps you discover what your child may be looking at online, and how to keep them safe with useful guides and online safety updates. Simply follow the link to access the Online Safety Hub:

https://theeducationalliance.onlinesafetyhub.uk/

- Text Message 2 - Qustodio Premium Online Safety Parent App

Parent, create your FREE Qustodio account to protect your children's devices:

https://www.qustodio.com/en/30-days-school-special/?utm_source=internal&utm_medium=OSHub&utm_campaign=theeducationalliance

Get more visibility on what's going on in your child's online world and make sure they are kept safe online. Block dangerous content, introduce screen-free schedules, receive alerts for inappropriate content and more.

---

4. Links to Online Safety Hub Articles

Please see below links to articles that feature on the Online Safety Hub.

Simply find your topic of interest (there are 30+) in the table below, copy the resource link we've already pulled from the Online Safety Hub, and share it via SMS, email, social media, or any other channel you use to communicate with your parents and carers.

Share this with other relevant members of your community or school staff, particularly those involved in parent communication. To make collaboration easier, feel free to utilise the "Date to be distributed" column.

For additional support, please contact:

Katherine Howard, Head of Education and Wellbeing Katherine.Howard@smoothwall.com

Resource	Link	What is the resource about?	Date to be distributed (WC)
Qustodio			
Qustodio - Parental Controls	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/qustodio-parent-app	Qustodio world learning online safety tool that helps parents manage and supervise their children's online activities	19/9/25
Getting started with Qustodio	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/getting-started-with-qustodio	Getting started with Qustodio - Instructions to support families in using Qustodio	26/9/25
Managing Youtube with Qustodio	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-to-manage-youtube-with-qustodio	Information to support families using Qustodio	3/10/25

Using Qustodio to block inappropriate content	https://theeducationalalliance.onlinesafetyhub.uk/parent/videos/blocking-inappropriate-content-with-qustodio	Blocking inappropriate content with Qustodio - Video	10/10/25
Parental controls			
Parental controls - Navigating the need	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/navigating-the-need-for-parental-controls	Navigating the needs for parental controls	17/10/25
Social Media			
Navigating social media and gaming safely	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/navigating-social-media-and-gaming-apps-safely	Supporting families to discuss how to keep their children safe online using our ABC model.	24/10/25
Safe Chat : The best messaging apps for children	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/safe-chat-the-best-messaging-apps-for-children-1	A good place to start for messaging apps.	7/1/25
Snapchat	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/snapchat	Review of the snapchat platform Information, advice and guidance for parents	15/5/26
Tiktok	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/tiktok	Review of Tiktok Information, advice and guidance for parents	22/5/26
Instagram	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/instagram	Review of instagram - Information, advice and guidance for parents	5/6/26
Discord	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/discord	Review of Discord - Information, advice and guidance for parents	12/6/26
The prevent duty - advice and support for parents	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/the-prevent-duty-advice-and-support-for-parents	Information and advice relating to the prevent duty.	14/11/25

Gaming and Apps			
Unlocking the lid on loot boxes	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/unlocking-the-lid-on-loot-boxes-1	Information, advice and guidance for parents relating to loot boxes.	
Location-tracking apps : Spying or good parenting?	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/location-tracking-apps-spying-or-good-parenting-	Information, advice and guidance for parents relating to location tracking app and things to consider.	
Digital wellbeing			
The ABC model for digital safety and wellbeing	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/the-abc-model-for-digital-safety-and-wellbeing	The ABC model for creating a safe environment includes 3 key steps. Access, Boundaries and Communication.	24/10/25
Parenting advice			
How sharenting influences your child's online identity.	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-sharenting-influences-your-child-s-online-identity	Supporting families to explore their understanding of sharenting.	21/11/25
The VPN vanishing act	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/the-vpn-vanishing-act-how-tech-savvy-teens-trick-parental-controls	Supporting families to understand the use of VPN's.	28/11/25
Modelling healthy digital habits to your children	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/modelling-healthy-digital-habits-to-your-children	Supporting families to explore their understanding of healthy digital habits and the importance of modelling their behaviours.	5/12/25
	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/modelling-healthy-digital-habits-to-your-children		5/12/25
The Anxious generation :	https://theeducationalliance.onlinesafetyhub.uk/parent	The Anxious Generation makes	

Trending research from online safety experts	/articles/modelling-healthy-digital-habits-to-your-children	a number of important observations about the changing faces of childhood and parenting in the modern world.	12/12/25
Online Bullying FAQ	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/online-bullying-faqs	Support for families to support with this challenge	9/1/26
Managing online safety in co parent families	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/managing-online-safety-in-co-parent-families	Information and support to manage online safety in co parent families	16/1/26
Predators			
How predators persuade children to send explicit images	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-predators-persuade-children-to-send-explicit-images-1	Support for families relating to predators on the internet.	30/1/26
Dealing with exposure to pornography online	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/dealing-with-exposure-to-pornography-online	Support for families regarding exposure to pornography online	6/2/26
Online Grooming : The red flags to watch for	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/online-grooming-the-red-flags-to-watch-for	Support for families relating to predators on the internet.	13/2/26
Bullying			
Three steps to navigating online nastiness	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/three-steps-to-navigate-online-nastiness-1	Support for families relating to predators on the internet.	16/1/26
How to report incidents on messaging apps	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-to-report-	If you ever find your child facing abuse or unwanted contact online, there are	23/1/26

	incidents-on-messaging-apps-1	useful tools at your fingertips to help manage the situation.	23/1/26
Safety			
How to spot fake online accounts	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-to-spot-fake-online-accounts	Support for families regarding fake online accounts	27/2/26
How to tackle online impersonation	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/how-to-tackle-online-impersonation	Online impersonation accounts are often created for negative reasons, including bullying, incitement of violence, or making inappropriate remarks, but children create them as an act of retribution or as a 'joke,' contributing to the persistence of this issue despite improved identity verification measures.	6/3/26
Money Management apps for children	https://theeducationalliance.onlinesafetyhub.uk/parent/articles/dollars-sense-money-management-apps-for-children-1	Support for families relating to money management	13/3/26
Generative AI			
AI safety tips with Qustodio	https://theeducationalliance.onlinesafetyhub.uk/parent/videos/ai-safety-tips-with-qustodio	AI offers exciting opportunities however it also poses potential risks that parents need to be aware of.	26/3/26
Character Ai	https://theeducationalliance.onlinesafetyhub.uk/parent/reviews/character.ai	Apps review on Character Ai	17/4/26

Apps reviews			
Minecraft	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/minecraft	Support for families relating to Minecraft	20/3/26
Pixel Wars - Minecraft vs Roblox	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/pixel-wars-minecraft-vs.-roblox	Information for families relating to minecraft and roblox and things to consider	
Online Gaming FAQs	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/online-gaming-faqs	Information relating to gaming and the common questions families have relating to gaming	
Roblox	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/roblox	Support for families relating to Roblox	
Among Us	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/among-us	Support for families relating to Among Us	
Steam	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/steam	Support for families relating to Steam	
YouTube	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/youtube	Support for families relating to YouTube	
WhatsApp	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/whatsapp-messenger	Support for families relating to WhatsApp	
Messenger	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/messenger	Support for families relating to Messenger	

Snapchat	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/snapchat	Support for families relating to Snapchat	
Instagram	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/instagram	Support for families relating to Instagram	
Discord	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/discord	Support for families relating to Discord	
Amazon	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/amazon	Support for families relating to Amazon	
Call of Duty Mobile	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/call-of-duty-mobile	Support for families relating to COD mobile	
Netflix	https://theeducationalalliance.onlinesafetyhub.uk/parent/reviews/netflix	Support for families relating to Netflix	
Privacy			
Unmasking the world of digital disguise	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/unmasking-the-world-of-digital-disguise	Support for families on fake accounts and catfishing	24/4/26
Location tracking apps - Good or bad ?	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/location-tracking-apps-spying-or-good-parenting-	Information relating to location tracking apps and their use.	1/5/26
Tops tips to protect your child’s digital privacy	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/top-tips-to- protect-your-child-s-digital- privacy	Top tips to protect your child’s digital privacy	8/5/26
Screentime			
The power of the internet filtering for online safety	https://theeducationalalliance.onlinesafetyhub.uk/parent/articles/the-power-of-	Information for families on how to use internet filtering for online safety	

	internet-filtering-for-online-safety-1		19/6/26