



Online Safety Policy

Policy:	Online Safety Policy
Last reviewed:	September 2026
Date of next review:	September 2027 (In line with KCSIE Updates)
Reviewed by:	Heartwood Computing Subject Lead
Approved by:	Executive Headteacher

1.0 Introduction

This policy should be read in conjunction with other relevant School, Federation and County Council policies, procedures and Codes of Conduct including:

- Safeguarding (Child Protection) Policy
- School Capability/Conduct Policies
- Social Media Policy
- Staff Acceptable Use Policy
- Pupil Acceptable Use Agreement
- Relationships (Behaviour) Policy
- Anti-Bullying and Anti-Hate Policy

All staff must be familiar with this policy and associated policies listed above, and all staff and pupils must sign the relevant Acceptable Use Policy/Agreement before being allowed to access school's systems. As Online Safety is an important part of strategic leadership within the school and Federation, all staff have a shared responsibility to ensure that policy and practices are embedded.

Safeguarding all stakeholders; children, members of staff, governors and volunteers, is at the forefront of everything we do. We are aware however, that certain children, such as those unsure of their sexual orientation, those on the autistic spectrum and those experiencing mental ill health, are at increased risk online. The Federation recognises that some children may be at greater risk of online harm, including children with SEND, children with medical needs, young carers, looked after and previously looked after children, children with social workers, children experiencing mental ill health, children vulnerable to exploitation and children experiencing prejudice-based harm.

As a Church Federation, we identify Christian values that underpin the whole of our community. These values inform our schools' vision, aims and ethos, the design of our curriculum, all policies, planning and the schools' management and governance. The values that relate particularly to this Policy are Trust, Respect and Love.

1.1 Staff should be given sufficient training and knowledge to be able to recognise and report potential online safety incidents as well as to teach and equip children to stay safe online.

1.2 It is the intention of the policy to ensure that staff and children act responsibly and safely online and that staff know procedures in place, when reporting potential online safety issues. This policy describes the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practices embedded in our schools and followed by the whole federation community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, preventing and responding to online safety incidents
- A progressive, age-appropriate e-safety curriculum for all pupils

2.0 – Online Safety Overview and Definition

At Heartwood Federation, we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.



The use of these exciting and innovative technology tools in school and at home, have been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '4 C's' Contact, Content, Conduct and Commerce which are outlined in Keeping Children Safe in Education and may include:

• **Content:**

1. being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, misinformation, disinformation, racism, faith-based abuse, sexism, misogyny, misandry, homophobic or biphobic abuse, discriminatory bullying, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'. This may also include harmful interactions with generative AI systems and chatbots.

• **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, including AI-generated sexual imagery, deepfakes and deep nudes. sharing other explicit images and online bullying.

• **Financially Motivated Sexual Extortion (Sextortion):** Children may be pressured into sharing nude or semi-nude images and subsequently blackmailed for money, bank details, gift cards or further images. Any concerns relating to sextortion will be treated as safeguarding concerns and dealt with in line with the Federation's Child Protection and Safeguarding Policy.

• **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>). Children may also be vulnerable to financially motivated sexual extortion (sextortion), whereby images are used to coerce victims into making payments or supplying personal information.

1. Children may also experience prejudice-based online harm, including racism, faith-based abuse, sexism, misogyny, misandry, homophobic abuse, biphobic abuse and other forms of discriminatory bullying. Staff should recognise that such behaviours may constitute safeguarding concerns and should be responded to in accordance with the Federation's safeguarding procedures.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online Safety issues can also affect adults who work at or are associated with the school and this will be referenced in more detail later in this policy.

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

3.0 Technology

Technologies regularly used by pupils and staff include:

3.1 Staff:



- Staff laptops, tablets, desktops, server access and access to SIMS systems. Staff laptops and tablets can also be used at home in accordance with the Staff Acceptable Use Policy (AUP).
- Curriculum tablets for preparing and delivering pupil activities.
- Visualisers, class cameras and other peripherals such as interactive whiteboards.

3.2 Pupils:

- Curriculum tablets, laptops including filtered access to the Internet and pupil level access to areas of the school network.
- Cameras and peripherals including programming resources (Beebots, Microbits etc.)

Please see Appendix 2 which outlines our expectations for pupils use of technology in school.

3.3 Where the school/federation changes the use of existing technology, or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

4.0 AI

Artificial Intelligence (AI) is increasingly being used across education to support teaching, learning, and administration. Heartwood Federation recognises the opportunities AI presents for enhancing efficiency and innovation. However, AI must be used in a safe, ethical, and responsible manner, ensuring compliance with safeguarding, data protection, and academic integrity principles.

This policy must be used in conjunction with the Acceptable Use Agreement for both Staff and Pupils and Parents/Carers which states clear expectations for AI use.

Roles and Responsibilities in regard to AI

Effective oversight and accountability are essential to ensure AI is used appropriately and safely within the school. The following sections define the key responsibilities of school leadership, staff, students, and IT teams in managing AI systems.

• Leadership and Governance

School leadership plays a vital role in overseeing AI governance, ensuring policies align with national regulations, and implementing best practices for safe and ethical AI use.

- Ensure AI governance aligns with DfE, KCSIE, and GDPR regulations.
- Approve AI tools before they are used in teaching, learning, or administration.
- Conduct annual AI risk assessments and policy reviews.
- Ensure AI use is transparent, fair, and free from bias.
- Leadership and Governance teams must engage in annual update training to ensure compliance and risk mitigation for the latest risks.

• Teaching and Support Staff

Teachers and support staff are responsible for ensuring AI is used as an educational aid while maintaining academic integrity, supporting student learning, and preventing misuse.

- Use AI as a teaching aid, not as a replacement for pedagogy.
- Verify AI-generated content for accuracy, appropriateness, and bias.
- Educate students on AI literacy, misinformation, and deepfakes.
- Ensure AI use does not compromise academic integrity or safeguarding.



- Teaching and Support staff must engage in annual update training to ensure compliance and risk mitigation for the latest risks.

- **Pupils**

Pupils at Heartwood Federation are, in most circumstances, not to use AI in any capacity unless in a situation supervised and planned by a member of staff.

- **Other Considerations**

AI should be implemented in ways that are fair, transparent, and aligned with ethical considerations. This section outlines the key principles for ensuring AI use remains accountable, unbiased, and secure.

It is essential that AI use within the school remains transparent, and that decisions made using AI are documented and subject to human oversight.

- AI must not be used to make independent decisions affecting students or staff.
- The use of AI in assessment, recruitment, or administrative decision-making must be documented.
- AI-generated content must be identified where used.

AI systems must be reviewed and monitored to minimise bias, ensuring fairness in learning, assessment, and administrative decision-making.

- AI tools must be vetted to ensure fairness and prevent bias.
- Training must be provided to recognise AI bias and hallucinations and mitigate its impact.
- Human checking is required for all AI output.
- All stakeholders are responsible for any output shared that has been generated by AI.

AI, Safeguarding and Online Safety

AI must be used safely within the school environment, preventing harm and ensuring students and staff understand the potential risks associated with AI-generated content.

Preventing AI-Generated Harm

AI-generated content, including deepfakes and misinformation, presents new safeguarding challenges. Staff and students must be aware of these risks and trained to respond appropriately (annually at a minimum).

- AI tools must not be used to create harmful, misleading, or inappropriate content.
- Students and staff must be trained to recognise AI-generated deepfakes, misinformation, and impersonation risks.

Staff should also be aware of AI-generated child sexual abuse imagery, deep nudes, AI-enabled fraud, phishing and financially motivated sexual extortion.

Additional AI Risks

Staff and pupils should understand that AI may be used to:

- generate deepfake imagery
- create deep nude images
- impersonate trusted adults
- support grooming activity
- spread misinformation and disinformation
- create manipulated child sexual abuse imagery
- facilitate fraud and sextortion



5.0 The Online Safety Curriculum

Teaching and learning around online safety forms part of The School/Federation's rolling Computing curriculum and is regularly taught and revisited (termly).

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age-appropriate e-safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- At KS1: use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- At KS2: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

The eight core strands from 'Education for a Connected World' (DfE) suggest that the curriculum should cover 8 main strands being:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

In correlation with the PSHE curriculum, pupils will be taught at an appropriate level about:

- misogyny
- online influencers
- deepfakes
- pornography
- nudes and semi-nudes
- consent
- harmful sexual behaviour

At Heartwood Federation, we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that through guided experience, children will learn safe life-long online behaviours.

This is achieved using:

- The Gloucestershire School's Partnership's (GSP) Digital Futures curriculum document;
- Discrete and embedded activities drawn from a selection of appropriate materials e.g. Google Be Internet Legends, Childnet and CEOP video resources (also referenced in Digital Futures);

Our programme for e-safety education is outlined in our Computing Curriculum Progression document and curriculum documentation.



Key online safety messages are also delivered and reinforced through cross curricular opportunities such as researching, blogging and communicating online, using a variety of media. Online safety messages are also delivered through worships and assemblies when appropriate.

6.0 Continued Professional Development

Heartwood Federation schools are members of the Gloucester Schools Partnership (GSP) and GLOSSI. The Computing Subject Leaders of member schools, meet regularly to discuss developments within the subject. Online Safety forms a large part of these discussions.

- New staff receive information on the school's Acceptable Use Policy as part of their induction, including advice on protecting their professional reputation online.
- All staff have to confirm that they have read and understood our Staff Code of Conduct and Relationships (Behaviour) Policy. They are also signposted to our Online Safety and Anti-Bullying and Anti-Hate Policy.
- Staff at Heartwood Federation receive up-to-date information and training on Online Safety issues in the form of staff meetings and updates from Computing Subject Leader/Designated Safeguarding Lead/PSHE Subject Leader, as well as training from external providers, such as the police, where appropriate.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- Training will include emerging technologies, AI, deepfakes, sextortion, filtering and monitoring responsibilities and prejudice-based online harm.

7.0 School / Federation Websites

Schools are required to publish certain information online – which in practice means you must have a school website. You are not however, required to develop a website policy but sometimes the boundaries of responsibility for setting up, maintaining and ownership of the content are blurred and this can lead to difficulty.

The main purpose of our school website is to provide information. Our Federation/ schools' website will not only tell the world that our school exists, but it will provide information to our pupils and parents, promote the school to prospective pupils and families and publish the statutory information required by the Department for Education.

In conjunction with a range of online services, a school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Headteachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

The school has clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.



8.0 Monitoring, and Averting online safety Incidents

The Federation keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity, and reporting incidents, including following child protection procedures where appropriate.

The technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by ICT support through an external provider.

Safeguards built into the school's infrastructure include:

- Secure, firewalled internet
- Anti-virus software on all devices
- Secure staff email and data management; maintained by an external provider.
- Restrictions on download of software, apps and file types -an administrator password is required for this purpose.

Safeguards relating to staff include:

- Staff having their own, password protected logins to ICT systems and using 2FA.
- The schools' networks can either be accessed using a wired or wireless connection. However, the wireless network is encrypted and password protected. Key members of staff know and can authorise the wireless password to be used on new devices.
- School staff must ask permission to connect personal devices to the schools' wireless networks and obtain the Wifi password from SMT.

Safeguards relating to pupil use include:

- Staff monitoring pupils' use of technology and, specifically, the internet.
- Pupils' use of online services (including the World Wide Web) are supervised in school at all times.
- Pupils have their own logins.
- Heartwood Federation seeks to maintain its schools as mobile-phone-free environments. Pupils may not access personal mobile devices during the school day unless authorised by a member of staff for an agreed educational, medical or safeguarding reason.
- Pupils' personal devices must not be connected to the school's wireless network unless specifically authorised by senior leaders.
- Staff use of personal mobile devices must comply with the Staff Code of Conduct, Staff Acceptable Use Policy and safeguarding procedures. Staff must ensure that personal devices are used professionally and do not compromise safeguarding, confidentiality or data protection requirements.
- Secure, firewalled internet
- Anti-virus software on all devices
- Secure staff email and data management
- Restrictions on download of software, apps and file types

Cyber Security

Cyber security forms an important part of the Federation's safeguarding arrangements. The Federation will:

- Implement Multi-Factor Authentication (MFA) where available and appropriate.



- Maintain endpoint protection and anti-malware software on Federation devices.
- Provide cyber security awareness training for staff, including phishing and password security awareness.
- Work towards and maintain compliance with the DfE Digital and Technology Standards for Schools and Colleges.
- Maintain secure user access controls, ensuring users only have access to systems and information appropriate to their role.
- Regularly review cyber security risks and respond appropriately to incidents that may impact the safety, wellbeing or personal data of pupils, staff and the wider school community.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Filtering and monitoring effectiveness will be reviewed at least annually by the DSL, Computing Lead, Senior Leadership Team and ICT provider, with records retained.

9.0 Responding to Online Safety Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

Online safety concerns should not be viewed in isolation. Concerns identified through a child's online activity may form part of wider safeguarding issues, including child abuse, exploitation, neglect, child-on-child abuse, domestic abuse and Operation Encompass notifications. Staff should consider the wider context of any online safety concern and respond in accordance with the Federation's Child Protection (Safeguarding) Policy.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Federation staff will follow its agreed procedures for responding, including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's Acceptable Use Policies).
- Any online safety concern that may indicate abuse, exploitation or a child protection concern must be recorded on CPOMS and referred to a DSL immediately.
- All online safety concerns should be categorised appropriately on CPOMS and managed in accordance with the Federation's Child Protection (Safeguarding) Policy.
- *The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.* With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant Acceptable Use Policy (AUP) to incidents which occur outside of schools if s/he deems it appropriate.
- The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so. However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern with parents (where appropriate) before taking any further action. NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.



10.0 Roles and Responsibilities

As it relates to safeguarding, Filtering and Monitoring is everybody's responsibility. Clear roles, responsibilities and strategies however, are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

Governors

- Ensure they have overall strategic responsibility for filtering and monitoring gain assurances that the 'Meeting Digital and Technology Standards for Schools and Colleges' standards are being met.
- Identify and assign a member of the senior leadership team and a governor, to be responsible for ensuring the DfE 'Meeting digital and technology standards in schools and colleges' are met
- Identify the roles and responsibilities of staff and third parties, for example, external service providers (see below)
- Ensure that the filtering and monitoring provision is reviewed by leaders at least annually or when there has been a safeguarding risk

Senior Management Team

- Procuring a Filtering and Monitoring system which blocks harmful and inappropriate content (without impacting teaching and learning)
- Understanding the Filtering and Monitoring system
- Overseeing reports and analysing incident reports which are flagged
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of provision at least annually or when there has been a safeguarding risk
- Ensuring all staff understand their role; are appropriately trained; follow policies, processes; and procedures; and act on reports and concerns

Designated Safeguarding Lead

- Taking lead responsibility for safeguarding and online safety
- Maintaining oversight of emerging online risks including AI, sextortion, deepfakes and online harmful sexual behaviour.
- Ensuring regular checks are made to filtering and monitoring systems
- Overseeing and acting upon checks/ reports
- Respond appropriately to safeguarding concerns
- Working closely with Governors and the school's IT provider
- Reviewing the effectiveness of provision at least annually or when there has been a safeguarding risk

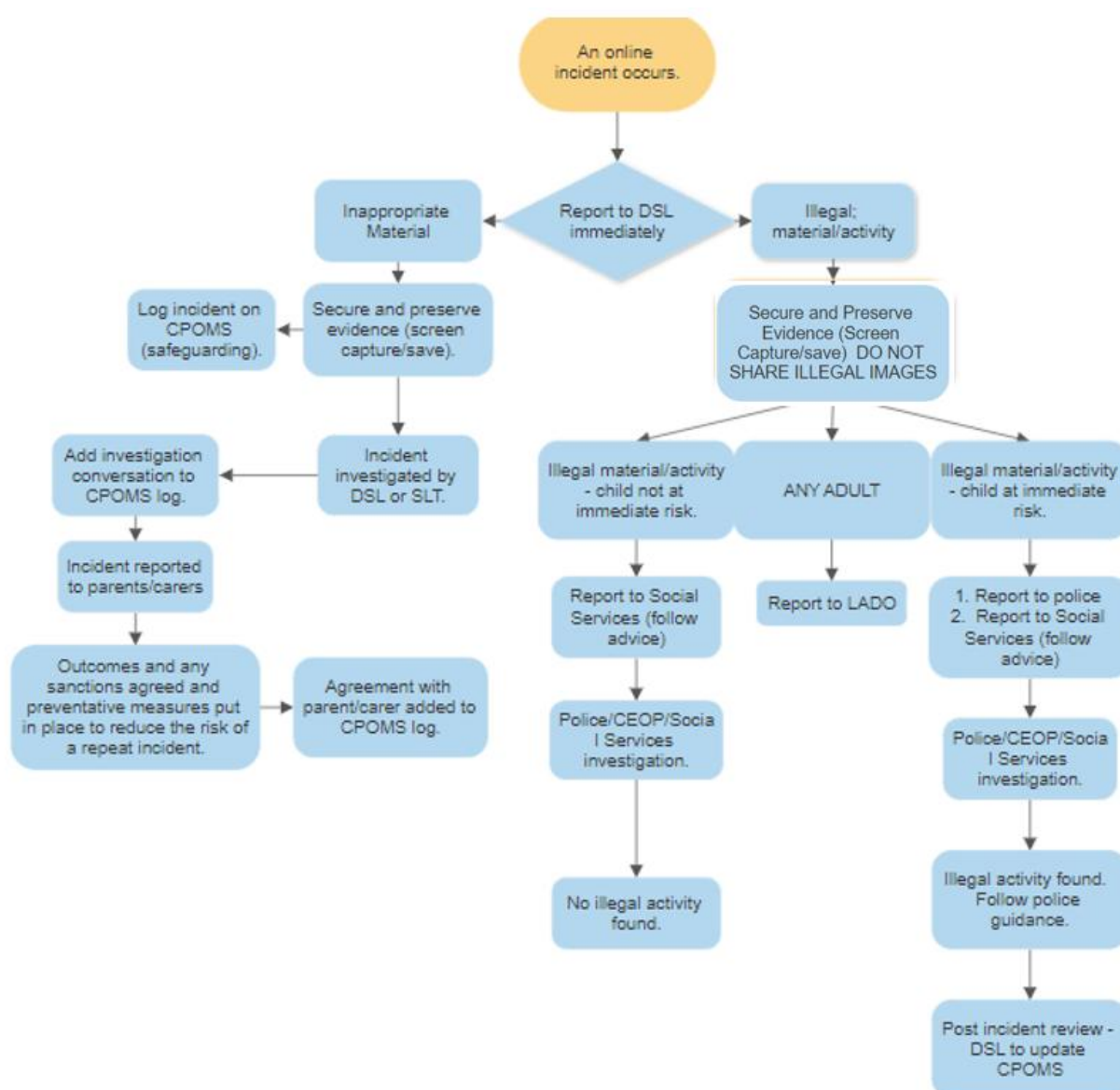
Technical Support

- Work with the Senior Leadership Team to procure a filtering monitoring systems, identify risk and carry out reviews and checks
- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Supporting Senior Management and the Designated Safeguarding Leads
- Completing actions following concerns or checks to systems

- Reviewing the needs of the school at least annually or when there has been a safeguarding risk (e.g. testfiltering.com or 360 safe), particularly ensuring it blocks illegal content. This should also be repeated should there have been an incident.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection and safeguarding procedures will be followed. *Please see Appendix 1 for usual procedures.*

Appendix 1- Response Procedure for an Online Incident



Incidents involving AI-generated imagery, deepfakes, deep nudes or financially motivated sexual extortion will be treated as safeguarding concerns and managed in line with KCSIE 2026 and the Child Protection Policy.

After any online safeguarding concern has been raised, filtering provision, effectiveness and settings will be reviewed.

POSH – Professionals Online Safety Helpline: 0344 381 4772

Appendix 2 - Advice for governing bodies/proprietors and senior leaders

- [Childnet](#) provide guidance for schools on cyberbullying
- [Educateagainsthate](#) provides practical advice and support on protecting children from extremism and radicalisation
- [London Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [NSPCC](#) provides advice on all aspects of a school or college's online safety arrangements
- [Safer recruitment consortium](#) "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- [Searching screening and confiscation](#) is departmental advice for schools on searching children and confiscating items such as mobile phones
- [South West Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [Use of social media for online radicalisation](#) - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an [Online Safety Audit Tool](#) to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) [Online safety guidance if you own or manage an online platform](#) provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) [A business guide for protecting children on your online platform](#) provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- [National cyber security centre](#) guidance on choosing, configuring and deploying video conferencing
- **Generative artificial intelligence (AI) in education (DfE)**
<https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>



Support for children

- [Childline](#) for free and confidential advice
- [UK Safer Internet Centre](#) to report and remove harmful online content
- [CEOP](#) for advice on making a report about online abuse

Parental support

- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Commonsensemedia](#) provide independent reviews, age ratings, & other information about all types of media for children and their parents
- [Internet Matters](#) provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [Let's Talk About It](#) provides advice for parents and carers to keep children safe from online radicalisation
- [London Grid for Learning](#) provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Stopitnow](#) resource from [The Lucy Faithfull Foundation](#) can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- [National Crime Agency/CEOP Thinkuknow](#) provides support for parents and carers to keep their children safe online
- [Net-aware](#) provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- [Parentzone](#) provides help for parents and carers on how to keep their children safe online
- [Parent info](#) from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

[UK Safer Internet Centre](#) provide tips, advice, guides and other resources to help keep children safe online

Understanding and Responding to AI-Generated Child Sexual Abuse Material (CEOP Education & Internet Watch Foundation)

<https://www.ceopeducation.co.uk/professionals/guidance/ai-guidance-for-professionals/>

UKCIS Online Safety Audit Tool



<https://www.gov.uk/government/publications/ukcis-online-safety-audit-tool>

Mobile Phones in Schools (DfE Statutory Guidance)

<https://www.gov.uk/government/publications/mobile-phones-in-schools>

