



Whiteheath Junior School Online Safety Policy

Written by (new policy)	Updated on	To be reviewed
Hannah Wells – September 2026		Autumn 2027



Introduction

Key people / dates

Whiteheath Junior School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Michelle Kenny – Headteacher Karen Padley – DSL/ Pastoral Lead
	Deputy Designated Safeguarding Leads / DSL Team Members	Hannah Wells – Deputy Headteacher
	Link governor for safeguarding & web filtering	Ali Percy – Chair of Governors
	Curriculum leads with relevance to online safeguarding and their role [PSHE/RSE/Computing leads]	Ashleigh Garland – PSHE/ RSE Lead Heather Malone – Computing Lead
	Network manager / other technical support	Paul Frimley – Inspire ICT
	Date this policy was reviewed and by whom	September 2026 – Michelle Kenny - Headteacher
	Date of next review and by whom	September 2027 – Michelle Kenny - Headteacher



What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE 2026), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review and amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place, why they are, and how the policy affects day-to-day practice. This policy should be read alongside our Acceptable Use Policy (updated September 2026). Any changes to this policy will be immediately disseminated to all the above stakeholders.

Who leads online safety?

KCSIE makes clear that "the Designated Safeguarding Lead should take **lead** responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not responsibility for this area, and whilst subject leads (e.g. for RSHE/ Computing) will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What were the main online safety risks in 2025/2026?

There are 4 types of online safety risks outlined in KCSIE:

CONTENT: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

CONTACT: being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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,



CONDUCT: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

COMMERCE: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is the responsibility of all staff to understand the above, recognise when a child may be experiencing harm related to the above, and report to the DSL.

Online Safeguarding Trends at Whiteheath Junior School

In our school over the past year, we have noticed the following in terms of device use and abuse and types of online/device-based incidents which could affect the wellbeing and safeguarding of our pupils: children inputting swear words in to a computer when they know it is inappropriate to use those words out loud, children typing messages to each other via a screen, e.g 'shut up', children searching for pictures/information about games which have a higher PEGI rating than their age.

How will this policy be communicated?

This policy can only impact upon practice if it is a living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available for all staff to download from a shared policy drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Sent to all staff when updated, all staff to sign to say they have read, have understood, and will adhere to. Records kept on file.
- Clearly reflected in the Acceptable Use Policy (AUP) which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school.
- Discussed in parent/carers workshops



Contents

Introduction	2
Key people / dates	2
What is this policy?	3
Who is it for; when is it reviewed?	3
Who leads online safety?	3
What were the main online safety risks in 2025/2026?	3
How will this policy be communicated?	4
Contents	5
Overview	6
Aims	6
Scope	7
Roles and responsibilities	7
Education and curriculum	7
Handling safeguarding concerns and incidents	9
Nudes & Semi Nudes	10
Upskirting	12
Bullying	12
Child-on-child sexual violence and sexual harassment	12
Misuse of school technology (devices, systems, networks or platforms)	12
Social media incidents	13
Extremism	13
Data protection and cyber security	13
Appropriate filtering and monitoring	14
Messaging/commenting systems (incl. email, learning platforms & more)	15
Authorised systems	15
Behaviour/usage principles of messaging/commenting systems	16
Use of generative AI	16
Online storage or learning platforms	17
School website	17
Digital images and video	17



Social media	18
Our SM presence	18
Staff, pupils' and parents' social media presence	19
Device usage	20
Personal devices including wearable technology and bring your own device (BYOD)	20
Use of school devices	21
Trips / events away from school	22
Searching and confiscation	22
Appendix A – Roles	23
All staff	23
Headteacher	24
Designated Safeguarding Lead	24
Governing Body, led by Safeguarding Link Governor	26
PSHE / RSE Lead	27
Computing Lead	27
Subject leaders	28
Network Manager	28
Data Protection Officer (DPO)	29
Volunteers and contractors	29
External groups including parent teacher associations (PTAs)	30

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Whiteheath Junior School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day,



regardless of device or platform, and that the same standards of behaviour apply online and offline.

- Facilitating the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
 - for the benefit of the school, supporting the school ethos, aims, and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

Scope

This policy applies to all members of the Whiteheath Junior School community (including teaching, supply and support staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to; behave respectfully online and offline, to use technology for teaching and learning, to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the school reputation. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

All members of the school community should **read the relevant section in Appendix A of this document** that describes individual roles and responsibilities. Please note that there is one for 'All Staff' that must be read by all staff, including those who have a named role in another section. There are also role descriptions in the Appendix A, e.g. pupil, governor, etc. All staff have a key role to play in feeding back on potential issues.

Education and curriculum



Despite the risks associated with being online, Whiteheath Junior School recognises the opportunities and benefits for children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

At Whiteheath Junior School, we engage our pupils in discussions about online safety and technology use during the children's weekly computing lessons, themed assemblies and days (such as Safer Internet Day) and their PSHE/ RSE learning. This helps us to ensure that our teaching of online safety is up to date and responsive to children's experiences and needs.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world responsibly, safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

The RSE Guidance states: "The curriculum should build knowledge and skills sequentially, with regular feedback provided on pupil progress. Lessons should ensure that all pupils are challenged, and assessments should identify where pupils need extra support or intervention."

The teaching of online safety, features in these particular areas of curriculum delivery:

- Relationships, sex and education (RSE)
- Personal, social, health and economic education (PSHE)
- Computing

Progression maps for knowledge and skills taught in the above subjects can be found on the school website. It is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology in school or setting as homework tasks, all staff will encourage sensible use, monitor what pupils are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. bias, disinformation, misinformation, and conspiracy theories), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. This is done within the



context of an annual online safety audit, which is a collaborative effort led by Michelle Kenny – Headteacher, Karen Padley – DSL, Hannah Wells – Deputy Headteacher, Ali Percy – Chair of Governors.

We utilise data from our safeguarding reports, filtering logs, monitoring captures, parent/carers complaints and other stakeholder feedback to inform our curriculum, so that we are constantly learning from concerns and being reflexive and responsive to the needs of our children.

We recognise that nationally, children with SEND are less likely to receive effective online safety teaching, but are more at risk of being a victim of harm caused online. Therefore at Whiteheath Junior School, we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children need to protect them from harm and prevent future online harm.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by publishing a list of school-approved websites on our school website. This includes hyperlinks for ease of access.

Handling safeguarding concerns and incidents

Online safety concerns are safeguarding concerns. They must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small they seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with recognition and response to online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policy
- Prevent Duty and Radicalisation Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security

This school commits to taking all reasonable precautions to safeguard pupils online, but the internet can never be 100% safe (as stated in KCSIE), and we recognise that incidents will occur both inside school



and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school).

Any suspected online risk or infringement should be reported to the DSL as soon as possible on the same day. The DSL will ensure that a record is made of the concern on CPOMS - this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

As per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

Any concern/allegation about staff misuse is always (as per any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the complaint is referred to the Chair of Governors and/or the LADO (Local Authority's Designated Officer). The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online safety incidents involving their children, Children's Services and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The following sub-sections provide details on managing particular types of concern.

Nudes & Semi Nudes

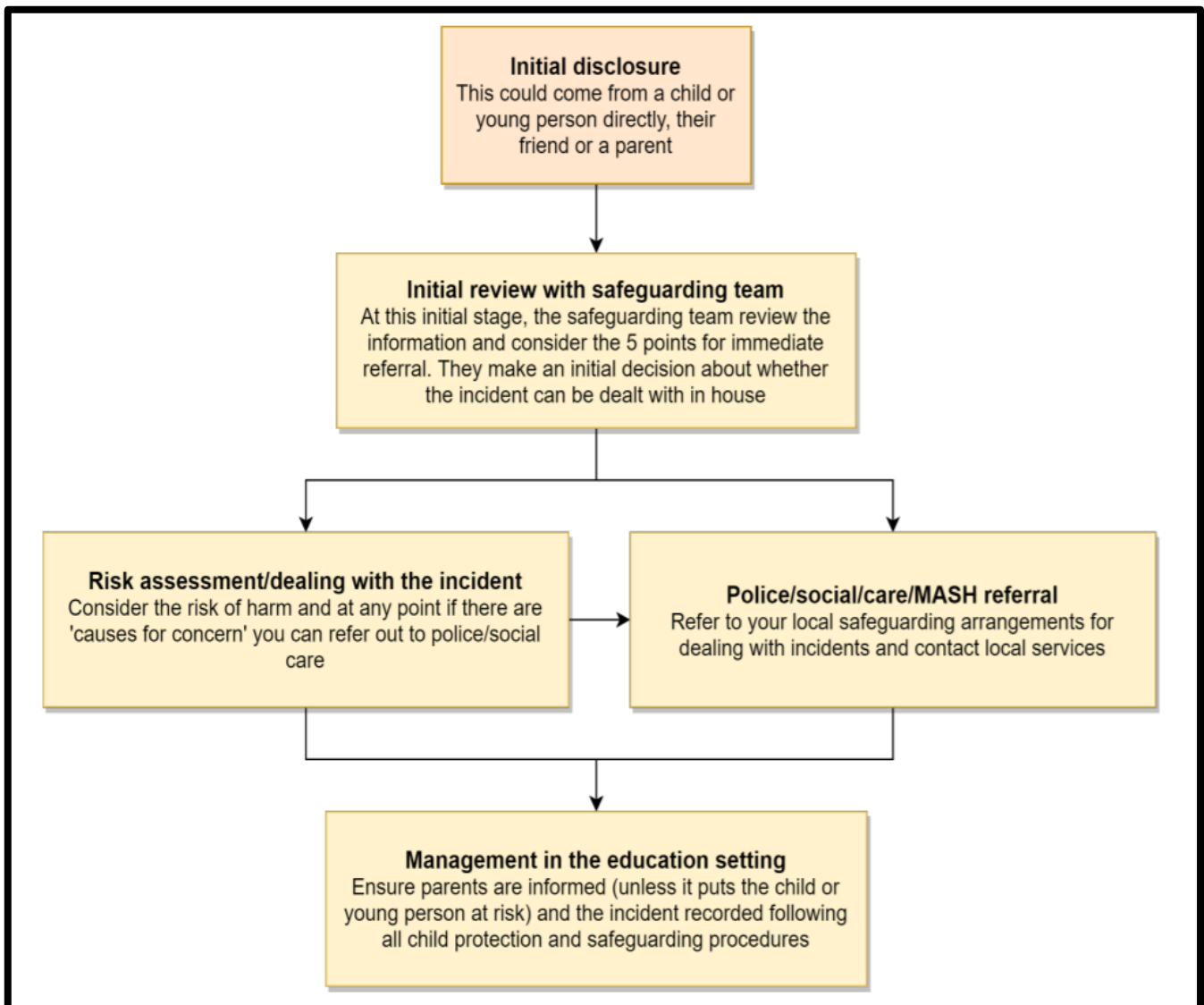
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance - [Sharing nudes and semi-nudes: advice for education settings](#).

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the Designated Safeguarding Lead (DSL) to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but go straight to the DSL.**

Everyone must understand that whilst the sharing of intimate or sexual images involving children (created via AI or otherwise) is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.



The school DSL will use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils. The school will also make use of guidance from [The Marie Collins Foundation](#) with regards to supporting victims of Technology Assisted Child Sexual Abuse.





This LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of sexual imagery of children:

SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?
A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm [...], suicidal or self-harming

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search.gov.uk

We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!

Upskirting

Everyone must understand that upskirting (taking a photo or video of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment, as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area. Upskirting has become more prevalent due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing. Wearable smart technology, such as smart glasses, or personal recording devices are not permitted in school (see Acceptable Use Policy).

Bullying

The school has a separate anti-bullying policy – this can be found on the staff shared drive and is published on the school website.

Child-on-child sexual violence and sexual harassment

This is a key area as outlined in KCSIE 2026 and the Ofsted School Inspection Toolkit (2026). This would be treated as a safeguarding concern and the safeguarding policy applied accordingly.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).



These are defined in the relevant Acceptable Use Policy as well as in this document, for example, in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where adults contravene these rules, action will be taken as outlined in the staff code of conduct.

It will be necessary to reinforce these as usual at the beginning of any school year, but also to remind pupils that the same applies to any home learning that may take place.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such where there are concerns of harm being caused, and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Whiteheath Junior School will request that the post be deleted and will expect this to be actioned promptly. The police may need to be contacted if an offence is committed.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the [Professionals' Online Safety Helpline](#), POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty – see the school Prevent Duty and Radicalisation Policy. Staff must not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be easily accessed and highly prevalent on mainstream platforms.

Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy/policies, which can be found on the staff policy shared drive. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE, which also refers to the DfE Standards of Cyber Security for Schools and Colleges.



Schools should remember that data protection does not prevent or limit the sharing of information for the purposes of keeping children safe.

Appropriate filtering and monitoring

The DSL has lead responsibility for filtering and monitoring, and works closely with Paul Frimley from Inspire ICT to implement the [DfE Filtering and Monitoring Standards](#).

We provide 'appropriate filtering and monitoring' (as outlined in KCSIE) in our school. Our filtering system is called School Protect. These systems are accredited by the UK Safer Internet Centre.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. We ensure all staff are aware of their responsibility in feeding back about areas of concern, potential for pupils to bypass systems and any potential over-blocking. Staff can submit concerns at any point by talking to the Headteacher.

Technical and safeguarding colleagues work together closely to carry out a full annual review and regular checks of filtering and monitoring, and to ensure that the school responds to issues, considers how to prevent further concerns and integrates with the curriculum.

We carry out monthly checks to ensure filtering is operational, functioning as expected, etc., and an annual review as part of an online safety audit of our approach. More details of both documents and results are available on request from Michelle Kenny - Headteacher.

Where staff use Gen AI, they must be pre-approved by the school. For children and young people, we block the generative AI category via our filtering and only allow specific pre-approved sites. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate/harmful content can be generated, so we carefully monitor output and limit their use (also in line with DfE guidelines).

Safe Search is enforced on any accessible search engines on all school-managed devices. Please note however that even with Safe Search enforced, AI is embedded in many search engine responses and this presents risk to users in terms of misinformation, bias, hallucinations and inappropriate content. Our YouTube mode is blocked for all children. This helps us to limit inappropriate content that is served to pupils.

The DSL checks filtering reports and notifications weekly (School Protect) and as and when SENSO alerts trigger an alert and takes any necessary action as a result.

According to the DfE standards, the school should have a plan for how to "monitor pupils when using school-managed devices connected to the internet. This is detailed in the filtering and monitoring policy.



At Whiteheath Junior School, we use LGfL Senso for monitoring. Monitoring alerts are received in real-time and are responded to (time scale depending on severity of concern).

Out of hours, our policies are:

- for filtering devices, the same filters would apply if staff were using devices remotely to access the school shared networks
- for monitoring devices, no monitoring takes places out of school hours.

Senso does not capture on staff accounts, but staff accounts are limited within the filtering restrictions. If a member of staff had an allegation about another member of staff, they speak to the Headteacher – Michelle Kenny.

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

Pupils at this school can receive communications from staff through Google Classroom. This is always posted publicly on a classroom's thread. Children cannot communicate with each other or members of staff – children do not have permission to post on Google Classroom. Children do have an 'email address' so that this could be used to generate them a username – they do not have access to this email inbox so cannot send/ receive communication via email.

Staff and governors at this school use the email system provided by LgFL for all school emails. They never use a personal/private email account (or other messaging platforms) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. This would be approved by the Headteacher, who may seek advice from our IT team.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If a private account is used for communication



or to store data by mistake, the DSL/Headteacher/DPO (the circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour/usage principles of messaging/commenting systems

- More detail for all the points below is given in the school's Acceptable Use Policy, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times by all users, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Staff are allowed to use the email system for school-related business (not excessive, not during lessons) and should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Use of generative AI

At Whiteheath Junior School, we acknowledge that generative AI platforms (e.g. ChatGPT, Canva, Co-pilot or Gemini for the creation of new text/imagery/code/music etc) are becoming commonly used by both children and adults. We are aware of and follow the [DfE's guidance](#) on this and we follow the subsequent principles:

- The use of any Gen AI in our setting (by staff or pupils) will be carefully managed by the school to ensure that users and their data are safe.
- Staff are only permitted to use their school email account when using pre-approved Gen AI, and they must not enter data relating to children, staff or the school which is personal or sensitive.
- The school has a clear and well communicated approach to the use of any Gen AI (by staff or pupils), and this is aligned with the school's values and pedagogical approaches.
- To help users to safely use technology, we will talk about the use of these tools with pupils, staff and parents – their practical use as well as their safety and ethical pros and cons.
- We are aware that there will be use of these apps and exposure to Gen AI creations on devices at home for many pupils – these experiences may be both positive/creative and also negative (e.g. data breaches, misinformation, bullying, deepfakes, creation of deepfake intimate imagery and chatbots that encourage unhealthy and inappropriate relationships). Therefore, it is important as a school that we support pupils in developing digital literacy skills to help mitigate these risks.



- In school, do not allow children to access Generative AI.
- Staff are able to use Generative AI to support with lesson planning or resourcing, but should ensure that all resources are appropriate and accurate before sharing with the children. Staff are not able to use Generative AI to upload pupil data or information – this is made clear in our Acceptable Use Policy.
- Should staff want/need to access a new platform, permission would need to be sought from the Headteacher who may take advice from other professionals or our IT provider.
- AI features in the Computing curriculum and ensures that pupils have an age appropriate understanding of AI and its uses.

Online storage or learning platforms

All the principles outlined above also apply to any IT system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. In Whiteheath Junior School this includes Collins Big Cat, Times Table Rock Stars, spag.com, Google Classroom, Scratch, Microbit, Nessy, and Tinkercad.

Any new platforms will be approved by the Headteacher.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the Office Manager/ Headteacher/ Deputy Headteacher.

The website is hosted by Juniper Education.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material must only be used with permission. Many open-access libraries of public-domain images/sounds, etc. can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with the Headteacher.

Digital images and video

Our approach to publishing imagery of pupils on our website/social media is that we do not upload high-resolution images of children. Photos are taken further away when possible, and group shots are used when appropriate.

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not



require express consent). The consent form stays with the child throughout their time in our school unless the parent/carers requests to make any changes.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Whiteheath Junior School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on a network drive (which is accessible by class teachers and SLT) in line with the retention schedule of the school's Data Protection Policy. The Deputy Headteacher is responsible for checking images/video on all school devices regularly. Any concerns about the nature of these images will be reported to the DSL.

Parents must **not** covertly film or record any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media, as there may be cultural or legal reasons why this would be inappropriate or even dangerous.

We encourage parents and children to think about their online reputation and digital footprint, and role model not oversharing on social media (or providing embarrassment in later life, and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be used and manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

Social media

Our SM presence

Whiteheath Junior School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.



Michelle Kenny - Headteacher is responsible for overseeing what is posted on our Instagram account – posts may be made by a senior leader or the Computing Lead, but are always checked by the Headteacher first. The commenting feature is disabled on all posts; separate photo consent has been obtained from parents/carers regarding their child's photos being used on Instagram. Direct messages are not responded to on Instagram as it is not an official communication channel.

Staff, pupils' and parents' social media presence

Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed – this is available for download on the school website. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 but the school sometimes deals with issues arising on social media – particularly WhatsApp - involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will explore online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents/carers can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

As outlined in the Acceptable Use Policies, pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.



Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such pupil accounts.

** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the school).*

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document that impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

Pupils

- Our approach to pupils using mobile phones is in line with the [DfE Guidance](#) . Pupils in Year 6 are permitted to bring a mobile phone to school (if a contract has been signed in advance) so they are able to contact parents/carers if making their own way to/from school. Phones are given in to the school office at the beginning of the day, locked in a secure box, and then returned to the child at the end of the school day. Any contraventions of this rule will be dealt with following the behaviour policy.
- Important messages and phone calls to or from parents can be via at the school office, which will also pass on messages from parents to pupils in emergencies.
- Personal recording devices, such as smart glasses, are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

All staff who work directly with children

- They should keep their mobile phones on silent and only use them in private staff areas (such as the staff room) during school hours. If a staff member is expecting an important personal call



when teaching or otherwise on duty, they need to make the Headteacher aware of this in advance.

- If staff need access to a mobile phone to manage a medical condition, this will have been discussed with the Headteacher in advance.
- Child/staff data should never be downloaded onto a private phone.
- Other personal recording devices such as smart glasses are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

Volunteers, contractors, and governors

- They should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this).
- Other personal recording devices, such as smart glasses are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

Parents/Carers

- They should ask permission before taking any photos and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events.
- We do not allow Apple AirTags or similar devices in school. Please note that it is against the terms and conditions of these products to use them to track a child.
- It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device. Other personal recording devices such as smart glasses are not permitted in school.

Use of school devices

School devices are not to be used in any way which contravenes AUPs, Behaviour Policy / Staff Code of Conduct.

Wi-Fi is accessible to visitors (such as SEND professionals, the facilities manager etc) for them to use on their own device. The password is not shared with these persons, a member of school staff will enter the password for them on their device. The device should only be used for school-related use whilst connected to the visitor WiFi and is subject to filtering.

School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, school devices should only be used for school-related tasks. Staff and pupils are



not permitted to use Virtual Private Networks (VPNs) on the school network or make any other attempts to bypass the school's filtering. Our filtering is set up to block all use of Virtual Private Networks (VPNs) on school owned devices and across the network.

Users should know that all and any usage of school owned devices, systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, teachers can be contacted on their personal mobile phones via the school office in case of emergency. Any communications to parents will be sent out via the school office or through the school website – never from a member of staff's personal mobile phone. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be reported immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure the number is hidden to avoid a parent or pupil accessing a teacher's private phone number.

Parents will be reminded that no devices owned by the children are ever to be taken on school trips or residential; including tracking devices such as Airtags. This is for the safety of all pupils.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example, as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.



Appendix A – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the “All Staff” section as well as any other relevant to specialist roles.

Roles:

- All Staff
- Headteacher
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSE Lead
- Computing Lead
- Subject leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors
- Pupils
- Parents/carers
- External groups, including parent associations

All staff

All staff should sign and follow the staff Acceptable Use Policy in conjunction with this policy, the school’s main Safeguarding & Child Protection Policy, the staff Code of Conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the Designated Safeguarding Lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring, and play their part in feeding back to the DSL about over-blocking, gaps in provision or pupils bypassing protections. All staff are also responsible for physically monitoring pupils’ online devices during any session/class they are working in.



Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Hillingdon Safeguarding Partnership support and guidance.
- Ensure the school implements and makes effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL— in particular, understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the Designated Safeguarding Lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Take overall responsibility for data management and information security, ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead

Key responsibilities (remember the DSL can delegate certain online safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should “take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure “An effective whole school approach to online safety” as per KCSIE.



- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out an annual review and regular checks on filtering and monitoring to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSE), ensure there is regular review and open communication, and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils is confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is updated annually.
 - This must include filtering and monitoring, and help them to understand their roles.
 - All staff must read and understand KCSIE Part 1 - translations are available in 13 community languages at
 - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates about online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSE guidance and beyond, in wider school life.
- Promote awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.



- Communicate regularly with SLT and the safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

Governing Body, led by Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#) .
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated annually.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated annually.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Governing bodies should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness at least once every academic year.
- Read all of KCSIE to ensure all governors understand their safeguarding responsibilities.
- Work with the DPO, DSL and Headteacher to ensure a compliant framework for storing data, helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Ensure all school staff have read Part 1 of KCSIE – governors are recommended to read ALL of KCSIE to ensure they fully understand their safeguarding responsibilities.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).
- “Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Ensure a whole school approach to online safety with a clear policy on the use of mobile technology.”



PSHE / RSE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed statutory [RSHE Guidance](#), including consent, mental wellbeing, healthy relationships and staying safe online, as well as raising awareness of the risks and challenges from the latest trends in generative artificial intelligence, financial extortion and sharing intimate pictures online, into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#), in an age-appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention through assessments, written assignments or quizzes, to capture progress" to complement the computing curriculum.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within PSHE / RSE.
- Develop and implement a RSE policy and publish this on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.



Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework 'Education for a Connected World' and 'Teaching Online Safety in Schools' can be applied in your context.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject policies refer to online safety/ filtering and monitoring arrangements.

Network Manager

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards, and remote-learning if necessary.
- Keep up to date with the school's online safety policy and technical information to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and any changes to these systems (especially access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.



- Manage the school's systems, networks and devices according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Monitor the use of school technology and online platforms; ensure that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO)

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not to prevent or limit the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "Data protection laws do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare."
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the Designated Safeguarding Lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per the AUP agreement, a contractor will never attempt to arrange any meeting, **including a tutoring/ support session**, without the full prior knowledge and approval from the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.



External groups including parent teacher associations (PTAs)

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within the school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.