

WIMBLEDON PARK PRIMARY SCHOOL

ONLINE SAFETY POLICY

Approved by Governors in October 2026

Next revision: October 2027

Introduction

Key people / dates

Wimbledon Park Primary School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Paul Lufkin
	Deputy Designated Safeguarding Leads / DSL Team Members	Esther Du Plooy, Lisa Kingsbury, Rachel Clement, Candice Stevenson, Sheerine Ahmed
	Link governor for safeguarding and web filtering	Milly Williams
	Network manager / other technical support	MM ICT
	Date this policy was reviewed and by whom	Sep 2026 (by SLT)
	Date of next review and by whom	Sep 2027 (by SLT)

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' 2024 (KCSIE), '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 or be integrated into your 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 should be a living document, subject to full annual review but also 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 it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the

responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks in 2026/2027?

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.

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and see in the context of the 4 Cs (see KCSIE for more details).

National Online Safeguarding Trends

1. LGFL SENSO MONITORING

The following are concerns highlighted through LGfL's partnership with Senso and monitoring data from LGfL schools. Many children are using Gen AI platforms on the school network and/or school devices, and the following have occurred:

- The creation of child sexual abuse material by and of children
- The spread of AI generated hoaxes, misinformation and disinformation. Sometimes these can be so realistic that it is difficult to determine what is true or not. One notable example of this was the sharing of fake information across social media about serious threats of violence in and between schools, which led to children/parents being fearful and some not attending school.
- Children turning to Gen AI platforms for advice – some of which is harmful and extremely worrying, e.g. dieting, relationships, bullying, and advice about self-harm
- Increased use of AI companions and chatbots which mimic human connection and have been seen to lead to AI induced psychosis, overuse, and heightened feelings of loneliness and shame. Tragically, there have also been numerous cases worldwide of children dying by suicide as a result of interactions with such bots.

There have also been numerous concerns related to staff use of Gen AI, including privacy and intellectual property breaches, and an increase in poor quality learning resources created using Gen AI.

Schools must address this, not just in the classroom, but by educating staff, governors, trustees, parents and pupils on safe use of digital technology, both for school and personal use. For guidance and resources, visit genai.lgfl.net.

LGfL Senso monitoring data has also revealed other concerns in schools:

- Children accessing inappropriate online games, dating sites and web chat where there is the risk of seeing adult and violent content and having interactions with strangers.
- The normalisation of violent and racist language between children, much of which doesn't suggest a particular ideology, but which could lead to extremism.

All these issues require a whole school approach to online safeguarding, as there is no quick or simple solution. It requires a combination of strong leadership, clear roles and responsibilities, robust policies and procedures, effective technical systems, highly competent staff who are regularly updated on this fast-paced world, effective and regular collaboration with parents, successful digital literacy and online safety teaching and more.

2. OFCOM'S LATEST RESEARCH

Ofcom's 'Children and Parents media use and attitudes report' published in 2026 has shown the following:

> *Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%. Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".*
>
> *Social pressures remain high, with 70% of students feeling pressure to be popular on social apps. Negative experiences are common; 23% of 8–17-year-olds personally experienced "nasty or hurtful" behaviour in the last year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).*
>
> *Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising. This suggests a need for updated curricula that reflect the evolving risks of AI and commercial influence.*

3. IWF, CSAM CONCERNS

Data from the IWF in their 2025 annual report highlights the scale of child sexual abuse imagery online. In 2025, the IWF assessed 451,210 reports, confirming that 311,610 contained child sexual abuse material (CSAM).

Schools should be specifically alert to emerging and persistent harms identified by the IWF, which include:

- Sexually coerced extortion (sextortion): Targeted threats against students – teenage boys in particular.
- AI-generated abuse: The use of generative tools to create non-consensual sexual imagery.
- Violence against women and girls (VAWG): A growing trend in digital spaces around violent and misogynistic narratives and language.

4. "COM NETWORKS"

A further concern highlighted by the National Crime Agency, is that of the existence of 'Com Networks'. These are networks of predominantly teenage boys, dedicated to inflicting harm and committing a range of criminality both on and offline, including cyber, fraud, extremism, serious violence, and child sexual abuse. The victims of these crimes are typically other children, some as young as 11, who have been coerced into seriously harming or sexually abusing themselves, siblings or pets. These networks are not hidden away in the dark web, but instead on platforms such as Discord, Telegram, Roblox, and Minecraft. Schools can help to protect children from these networks by enforcing effective filtering, training staff to recognise signs of exploitation, supporting parents to understand and mitigate the risks and building a curriculum that teaches students to identify grooming behaviours.

5. CYBER ATTACKS

Data from the Department for Science, Innovation and Technology (DSIT) states that 73% of secondary schools and 49% of primary schools identified a cyber breach or attack in the past 12 months (a significant jump from the previous year). Phishing remains the biggest entry point. AI is being used by scammers to generate sophisticated, error-free phishing emails targeting school administration and staff accounts. Schools are encouraged to ensure that they bridge the gap between technical understanding/cyber security policies, and operational understanding and practice.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) 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
- Summarised in the admin reminders document in September every year
- Part of induction for new staff
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff/adults in school and pupils with their parents (which must be in accessible language appropriate to these groups), which will be issued to school community, on entry to the school, annually and whenever changed, plus displayed in school

Overview

Aims

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

- Setting out expectations for all Wimbledon Park Primary 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 & 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 and Relationships Policy or Anti-Bullying Policy)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority Children's and Families Hub and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via **safetraining.lgfl.net**

Scope

This policy applies to all members of the Wimbledon Park Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/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 1 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

Schools must establish a carefully sequenced online safety curriculum that develops competencies (as well as knowledge of risks), that builds on what pupils have already learned, and identifies content appropriate for their stage of development.

Despite the risks associated with being online, we recognise 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, is critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

At Wimbledon Park Primary School we engage our pupils regularly and continually in discussions about online safety and technology use. 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.

RSHE guidance also recommends that schools assess teaching to "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 education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, 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.

Ongoing reviews of curriculum plans / schemes of work (including for SEND pupils) take place through weekly and termly planning and are used as an opportunity to follow this framework more closely in its key areas.

We utilise data from our safeguarding reports, filtering logs, monitoring captures, parental 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 [school name], 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.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE).

General concerns 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 err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour and Relationships Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, cyber security, image use etc)

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 reporting member of staff will ensure that a record is made of the concern on My Concern - 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.

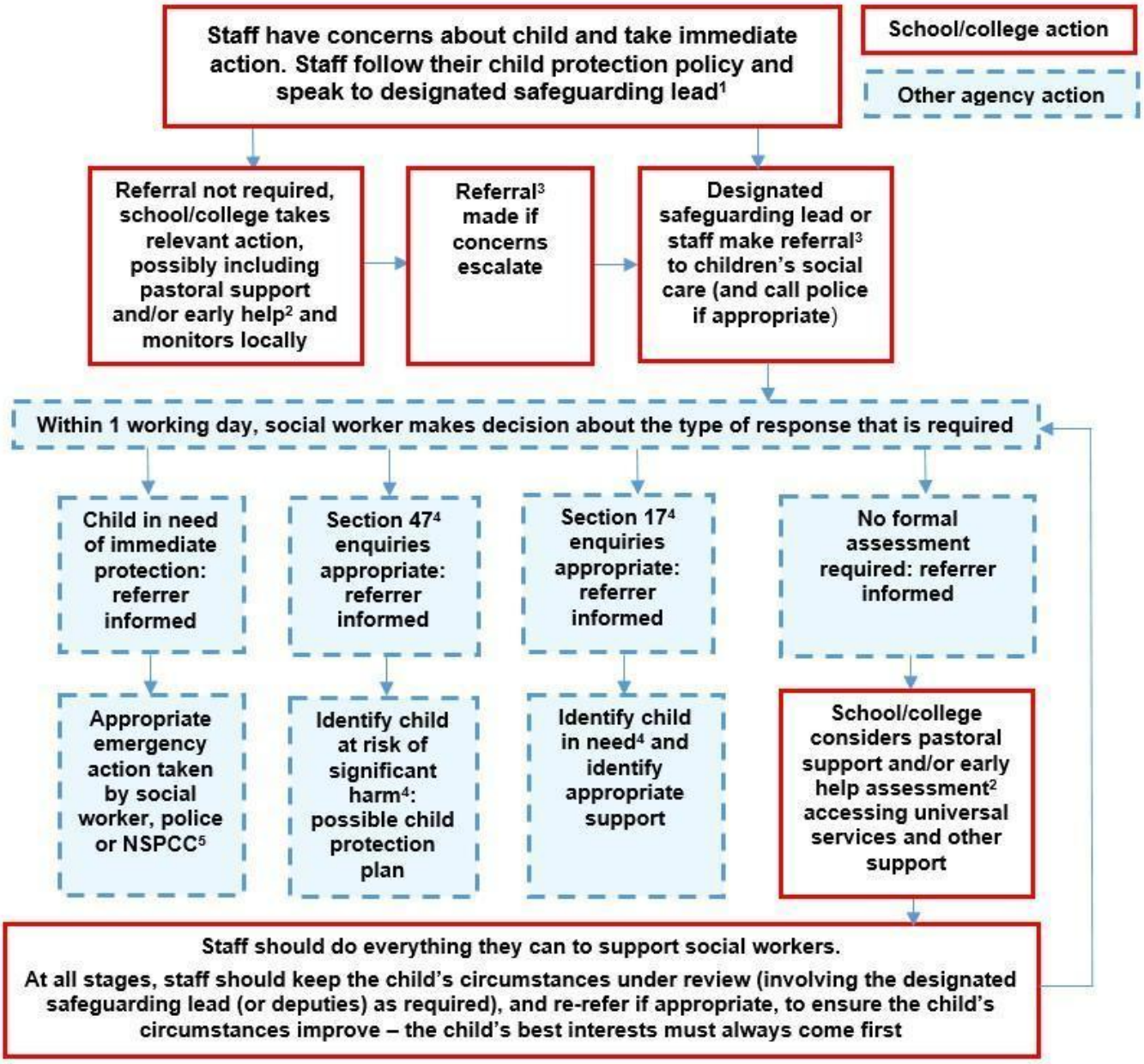
Any concern/allegation about staff misuse is always (as per any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the complaint is referred to the Chair of Governors and/or the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

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.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

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

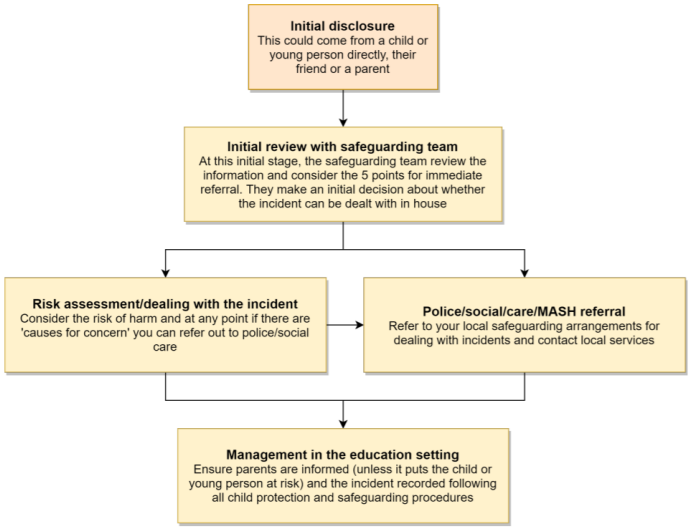
Sexting – sharing nudes and semi-nudes

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.

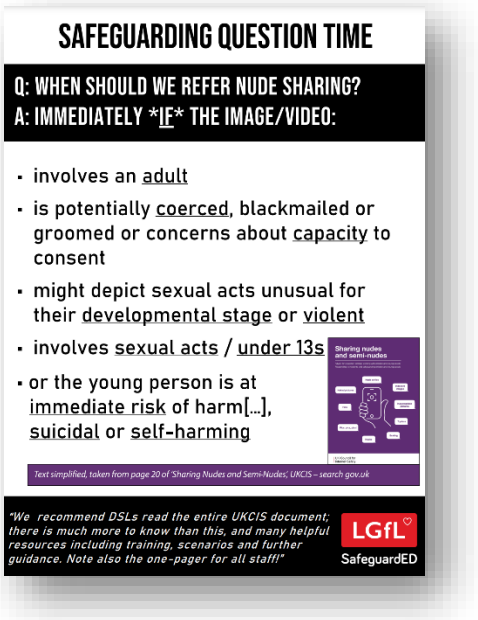
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the Designated Safeguarding Lead (DSL) to first become aware of an incident, and it is 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:



Upskirting

It is important that everyone understands that upskirting (taking a photo or video of someone under their clothing, not necessarily a skirt) is now 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/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

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 (see those for pupils in Appendix 2), 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 staff 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 for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

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

As of June 2026, the UK Government has announced that social media will be banned for under 16-year-olds.

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. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

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), Wimbledon Park Primary 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 – for support with this, please visit prevent.lgfl.net. 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 cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy. 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 designated safeguarding lead (Paul Lufkin) has lead responsibility for filtering and monitoring and works closely with MM ICT and DPO 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. This system is 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 overblocking. Staff can submit concerns at any point to Paul Lufkin, headteacher and DSL.

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

We carry out regular checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

Where staff use Gen AI, they must be pre-approved by the school. For children and young people, we block all generative AI

Safe Search is enforced on any accessible search engines on all devices.

Our YouTube mode is "Safety". This helps us to limit inappropriate content that is served to pupils.

The DSL checks filtering reports and notifications as notified and at least weekly 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."

At, we use LGfL Senso for monitoring all connected devises in school. The DSL receives live Senso notifications/alerts and takes any necessary action as a result.

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

Authorised systems

- Pupils at this school communicate with each other and with staff using G-Suite and LGfL London Mail
- Staff (and governors) at this school use the email system provided by LGfL (Staffmail) for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.
- Staff at this school use Bromcom to communicate with parents

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 with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.
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 this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below is given in the social media section of this policy as well as the school's acceptable use agreements, behaviour and relationships 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
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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

We acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.

Online storage or learning platforms

All the principles outlined above also apply to any 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.

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, Paul Lufkin, has Day-to-day responsibility of updating the content of the website and ensuring compliance with DfE requirements.

The site is managed by / hosted by Greenhouse School Websites.

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 only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with Paul Lufkin.

Digital images and video

Our approach to publishing imagery of pupils on our website/social media/marketing materials is as follows.

When a pupil/student 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) and for how long. Parents answer as follows:

- For displays around the school
- For use in school marketing

- For the website

And this information is recorded in Bromcom. Whenever a photo or video is used the member of staff taking it will check the consent status (in Bromcom) database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

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. The school provides staff with school iPads to capture images of pupils in school activities.

At Wimbledon Park Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils (but may capture images of classrooms and learning environments) unless authorised by the headteacher, in which occasional situations these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

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 (see nofilming.lgfl.net for more information). A sample letter to parents for taking photos or videos at school events can be found at saferesources.lgfl.net.]. Further information on managing pupil image and video content is available here.

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.

Staff, pupils' and parents' SM 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 would 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. 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 (and as of June 2026, the UK Government has announced that social media will be banned for under 16-year-olds), but the school regularly deals with issues arising on social media involving pupils/students 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 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). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentonlinesafety.lgfl.net and parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Email is the official electronic communication channel between parents and the school. Social mediais are not appropriate for school use. Parents are asked to follow guidelines for the use of email to communicate with teachers and guidelines for messaging in parent administrated class WhatsApp groups (see below).

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 public 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

Parent Communication Guidelines (shared annually in September)

Good communication and positive relationships between home and school are fundamental to a successful partnership with parents for their child's education and we are very fortunate at Wimbledon Park to work together with you in a very supportive environment with constructive and open communication.

Class teachers aim to keep you well informed about your child's learning and experience in school and this happens via the school website, meet the teacher evening, spring term parent consultation, SEND support plan meetings, Bromcom, informal meetings and phone conversations.

We hope that these channels provide the large majority of communication that parents need with their child's class teacher. However, there will also be circumstances where a need for a discussion or to share information with a class teacher arises outside of these usual channels, and class teacher emails can be a useful additional means of communicating. Email can also be useful to arrange a face to face or follow up telephone call.

Class teachers are busy. Their job is an intense one and they work long hours. Their priority focus is the children's education and they only have a small amount of time available to read and respond to emails.

We ask that parents use the following guidelines for emailing class teachers:

- Emails from parents to the class teacher should be primarily used for information sharing about children's learning, homework and any upsets or concerns that we need to know about
- Parent emails to school work best when they are brief and informative (less than 8 lines is appreciated)
- Emails should not be used to replace meetings or telephone calls where these are the more appropriate way of following up on queries/issues
- Teachers are not expected to respond to parent emails between 8:40 and 15:45 when they are teaching (and often they will be involved in after school training and meetings meaning they may not read and respond to emails until the following day)
- Please don't email teachers at the weekend or during school holidays
- Please contact the school office (and not the class teacher) to relay information about absence, collection arrangements, trip details, school clubs, lost property and other similar administrative matters.
- If you need to convey urgent information, please always email or telephone the school office in the first instance (copying the class teacher)
- If parents do raise a concern, an initial response or acknowledgment should usually be provided to parents within 24 hours (Monday to Friday). This will then be followed up in whatever manner is appropriate and agreed (which may include arranging an opportunity to find out more details)
- If the email relates to a concern or problem, it ought to be focused on understanding the problem and finding a solution (and not be assumptive, sarcastic, confrontational or accusatory)
- Emails should always be respectful and constructive as the tone and intent of email can easily be misunderstood (for example avoid using capital letters or bold text, or multiple exclamation marks)

We ask teachers to use the following automatic response to all external emails:

Thank you for your email. Your email has been received and will be read by your child's teacher at their earliest convenience. We are a school that prioritises teacher wellbeing and reduces unnecessary teacher workload. Please be mindful of the fact that teachers have very limited non-teaching time in which to read and respond to emails. You should not expect a response to emails about absence, collection arrangements, trip details, school clubs, lost property and other similar administrative matters. Please refer to the school website for information about school policies, clubs, and dates. Please look on Google Classroom for information about timetables, home learning, worksheets and information shared at the start of the year. Please also refer back to previous Bromcom communications. If the teacher feels a follow-up email or phone call is required regarding academic or wellbeing matters, they will contact you directly in the next 48 hours. For urgent matters please call or email the school office: info@wimbledonpark.merton.sch.uk

Teachers will forward parent emails to a member of the leadership team for support where the email doesn't meet the guidelines or where the issues raised are complicated and require leadership involvement.

Parent WhatsApp groups for classes/year groups are set up and coordinated by class reps. These groups are not operated or moderated by either the PTFA or the school.

We would ask that members follow these guidelines for messaging and those who do not follow these may be removed from their class group:

- WhatsApp groups are for timely reminders and information sharing about school/class events
- The information shared on these groups is not intended to replace Bromcom/other communications from the school.
- Please keep messaging brief, courteous and respectful.
- The group admins and class reps are not spokespeople for the school or class and their role is simply another parent in the group.
- Groups should not be used to share/air specific issues or grievances about other children in the class or about the school (for example, recently one parent inappropriately shared names and details of an incident between her child and another in class). Please raise issues and grievances directly and privately with the school/other party.
- Groups should avoid becoming discussion forums – the number of unwanted messages can rapidly spiral out of control. For example, discussion threads about the teacher strikes understandably generated a lot of parent reactions, but these WhatsApp groups are not the place to discuss matters like these.

Smartphone Free Childhood

At Wimbledon Park Primary School, we are proud to support the Smartphone-Free Childhood Campaign, an initiative dedicated to promoting healthier, happier childhoods free from the pressures of early smartphone use https://www.smartphonefreechildhood.org/about-us/our-mission

Research is showing us that smartphones and social media can have serious downsides for children and teenagers, such as:

- Impact on mental health (increased rates of anxiety and depression).
- Difficulty with attention and sleep.
- Risks of cyberbullying and exposure to harmful content (such as violent or inappropriate material).

- Addictive tendencies, which can pull children away from learning essential life skills.

The campaign was launched in response to growing concerns about the impact of smartphones on children's mental health, social development, and academic focus. Studies have shown that excessive screen time can affect sleep, reduce physical activity, and hinder the development of essential interpersonal skills. By encouraging a smartphone-free lifestyle for younger children, the campaign aims to foster creativity, curiosity, and meaningful connections with family and friends. Over 90% of 12-year-olds already have a smartphone! But the earlier children are exposed to smartphones, the greater the risks—especially during the vital years of brain development.

At Wimbledon Park Primary School, staff and governors are taking action. We are committed to maintaining a smartphone-free school environment around our children by:

- Asking staff not to use their phones in school at any time around children (unless in an urgent safety situation)
- Asking children not to bring any smartphone to school (if parents really want to track/communicate with their child to and from school, then we ask parents to buy a non-smart phone or use an air tag)
- Asking parents not to be on their phones when in the school playground

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)

- Our approach to pupils using mobile phones is in line with the DfE Guidance .
- **Pupils/students** at Wimbledon Park Primary School are allowed to bring mobile phones **that are not smart phones** to school for their journey to and from school. Children hand their phones to their teacher at the start of each day. Any attempt to use a phone in lessons without permission will lead to appropriate sanctions form the school's behaviour policy. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Some children may have watches that have the capacity to take images – these will be dealt with in the same way as use of mobile phones. 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** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone accessible to answer. Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off/on silent. 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 and this should be done in the

presence of a member staff. Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

- **Parents** are reminded and asked to adhere to the school being part of the Smart Phone Free Childhood campaign. Parents are asked to leave their phones in their pockets and turned off/ on silent when they are in school. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. 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 without written permission.

Use of school devices

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct. Wifi is accessible to all staff for their own devices within the framework of the acceptable use policy. Regular visitors (for example school nursing service or Jigsaw 4U counsellor) may request access to the school Wifi from Paul Lufkin. All and any usage of devices and/or systems and platforms connected to the Wifi network is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

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

Trips / events away from school

For school trips/events away from school, teachers used their own mobile phones for any authorised or emergency communications with pupils/students and parents. Teachers may want to ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Parents will be reminded about their child's permitted device use whilst on trips away from school, , including that tracking devices such as Airtags are not permitted 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.

Full details of the school's search procedures are available in the school Behaviour and Relationships Policy.

Appendix 1 – Roles and Responsibilities

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, including Safeguarding Link Governor
- PSHE Lead
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's safeguarding policy, the 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 and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher – Paul Lufkin

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead team
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children 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 / Online Safety Lead – Paul Lufkin

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. RSHE), 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
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that all governors undergo safeguarding and child protection training (including online safety) annually to enable them to provide strategic challenge and oversight into policy and practice
- 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 with the 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 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 RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') 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, 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 adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off-site, especially when in isolation/quarantine.
- 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 – Milly Williams

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
- 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.
- 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 […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

PSHE Lead – Jill Manning

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] tests, written assignments or self-evaluations, 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 / RSHE.
- Develop and implement a RSHE 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 – Paul Lufkin

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 RSHE 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 / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in their subject or aspect, especially as part of the RSHE 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 specific action plans also have an online-safety element

Network Manager/other technical support roles – MM ICT

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.
- 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 / RSHE 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.

- Support the Headteacher to ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Support the Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer (DPO) – SchoolPro TLC

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 (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety 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 AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil

Pupils

Key responsibilities:

Read, understand, sign and adhere to the student/pupil acceptable use policy

Appendix 2

LGfL SafeguardED

Acceptable Use Policy (AUP) for KS1 PUPILS

My name is _____

To stay **SAFE online and on my devices:**

1. I only **USE** devices or apps, sites or games if I am allowed to
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused
3. I look out for my **FRIENDS** and tell someone if they need help
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE**
6. Anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS** 🚫 unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES** ❌, even if someone tells me I must.
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** my personal information or other people's stories and photos
11. I am **KIND** and polite to everyone

My trusted adults are:

_____ at school

_____ at home

_____ at _____

My Online Safety Rules (KS2)

Being Safe

- **I will follow the school rules:** I will use school devices and the internet only when I am allowed and for schoolwork.
- **I keep passwords safe:** I will never share my passwords and will tell a teacher if someone else finds them out.
- **I check before I click:** I will not click on strange links that I do not know, or pop-ups without checking with a teacher, or parent/carer, nor download things without permission.
- **I respect age limits:** I will not use 13+ games or apps, as they are not safe for me.
- **I protect my identity:** I will not share private details like my address or phone number.
- **I can say no online if I need to:** I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I will say no, stop chatting and tell a trusted adult immediately.
- **I am a safe researcher**: I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across.
- **I don't livestream on my own**: I check with a trusted adult before I video chat with anybody for the first time.
- **We are a Smartphone Free School**: I do not bring a smartphone or other smart online technology into school

Being Kind

- **I am a good friend and ally:** I will not post or share unkind, rude, or hurtful messages, images, or videos. If a friend is worried or needs help, I remind them to talk to an adult, report it, or even do it for them.
- **I know what 'banter' means:** I know that calling someone names is not 'fun' or 'banter'—it can hurt people.
- **I don't take secret photos or videos:** I will not take pictures or videos of others without their permission. I will never create fake images, videos, or 'deepfakes' of anyone.
- **I respect work:** I only use other people's work (pictures or words) if I have permission.

Using Technology Responsibly

- **I check with an adult:** I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. I will talk to a trusted adult before chatting with anyone new, even if they claim to be a friend or are a 'chatbot'.
- **I know my body is mine:** I will not send photos or videos of myself or get changed in front of a camera. If I feel uncomfortable, I will stop and tell a trusted adult.
- **I don't pretend to be someone else:** I am always honest about who I am online.
- **I am careful what I share and protect my online reputation:** I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

What to do if something goes wrong

- **It's not my fault:** If I see something bad online or receive an unkind message, it is **not** my fault. I will not get in trouble for telling an adult.
- **I tell someone:** If I see or experience something that makes me feel worried, upset, or confused, I will stop what I am doing and tell a trusted adult straight away.

My Trusted Adults

At school, my trusted adult/s is/are: _____

At home, my trusted adult/s is/are: _____

I know I can also get in touch with Childline at 0800 1111

Signed: _____ **Date: _____**

Acceptable Use Policy (AUP) Social Story






What I Must do to Keep Safe Online and With Devices





Online means anything connected to the internet. Most devices and apps are

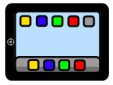



connected to the internet.





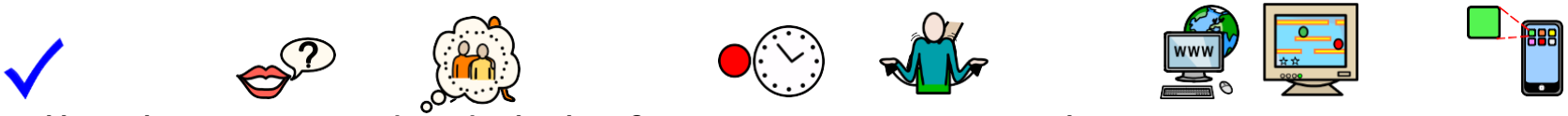
Devices are technology like: computers, laptops, games consoles,




tablets and smart phones.



I will only use the devices I am allowed to use.



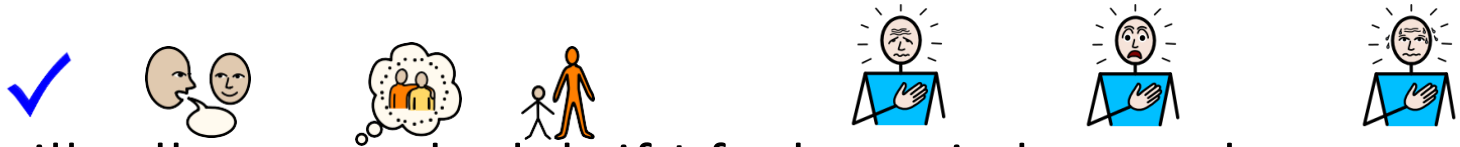
I will ask a trusted adult before I use new websites, games or apps.



I will ask for help if I'm stuck or not sure.



I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



I will tell a trusted adult if I feel bad or unsafe when I am using a device.








I know people online sometimes tell lies.





They might lie about who they are or where they live.



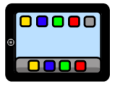



I never have to keep secrets from my trusted adults.









I will not change clothes or undress in front of amy camera.







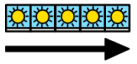

I will always ask a trusted adult before telling anyone my private



information or location.

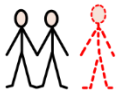






I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.




This could make me feel sad or embarrassed.





My trusted adults are _____ at school





My trusted adults are _____ at home




My name is _____