The King's Church of England Primary School

Encouraging every child to reach their full potential, nurtured and supported in a Christian community which lives and learns by the values of Love, Compassion and Respect.

THE KING'S SCHOOL
Online Safety and Acceptable Use Policy

Agreed by: FGB

Date: September 2024

Review Cycle: 1 year

Next Review Date: September 2025

Policy reviewed by FGB

Version 9

All the King's School policies should be read in conjunction with the Equality Policy

If you require a copy of this document

in large print, braille, audio format, or paper

please contact the School Office

Contents

Introduction

Key people / dates

The King's Church of England Primary School	Designated Safeguarding Lead (DSL) team	Ms K Verge (DSL) Ms T Demir (DSL) Ms T Sesay (DDSL) Ms P Watkinson (DDSL)
	Online-safety lead	Ms K Verge Ms T Demir
	Computing Lead	Ms S Carter
	Link governor for safeguarding/ Web filtering governor	Rev Melanie Harrington
	PSHE/RSHE lead	Ms M Huggins
	Network manager / other technical support	Mr A Rooney (SBM)
	Date this policy was reviewed and by whom	September 2024 Ms T Demir (DSL) Ms K Verge (DSL)
	Date of next review and by whom	September 2025 (DSL)

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 LGFL (London Grid for Learning), '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 our school's statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

At The King's School, we recognise the importance of digital learning in developing children's knowledge and understanding of the world around them. As such we are committed to ensuring pupils are provided with the skills to make the most of the ever expanding world of technology, therefore Computing is considered an essential part of our curriculum. The school is committed to the continuing development of our IT infrastructure and embracing new technologies to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

With our commitment to IT provision comes a responsibility to provide children with a safe environment in which to explore the technological world. As in other areas of life, children are vulnerable and may

expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities, which are inappropriate, or possibly illegal. In our commitment to online safety, The King's School seeks to address the issues around content, contact, conduct and commerce, and using these technologies safely to promote an awareness of the benefits and the risks.

Who is it for; when is it reviewed?

This policy is 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. This policy is updated at least annually and available alongside AUPs in the Appendix and at safepolicies.lgfl.net. Although many aspects will be informed by legislation and regulations, staff, governors, pupils and parents are involved in writing and reviewing the policy. This ensures all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see appendices) for different stakeholders help with this – 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.

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:

- The policy is posted on the school website and any issues regarding online safety are addressed in the school newsletter and on the safeguarding page on the website. This includes links to advice pages and other websites.
- Part of school induction pack for all new staff/ governors/ volunteers (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for:
    - Pupils – at the start of each year and reinforced in Computing lessons
    - Existing staff – annually in staff training
    - Existing governors – annually at full governing body meeting (FGB)
    - New parents – in EYFS starter packs or in new pupil induction packs
    - Existing parents – via website/ Arbor

What were the main online safety risks in 2023/2024?

Current Online Safeguarding Trends

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 seen in the context of the 5 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

Self-generative artificial intelligence has become rapidly more accessible, with many students often having unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information (gen AI can be responsible for incorrect and sometime harmful information), but also in terms of plagiarism for teachers and above all safety - none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home. Self-generative AI has also made it easier than ever to create sexualised images and deepfake videos. Whilst they may not be real, they have a devastating effect on a young person's emotional wellbeing and physical safety, and can also be used to blackmail, humiliate and abuse. The Internet Watch Foundation has reported AI-generated imagery of child sexual abuse progressing at such a worrying rate.

Ofcom's 'Children and parents: media use and attitudes report 2024' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further (especially with the minimum age for use of WhatsApp now 13). With children aged 3 - 17 spending an average 3 hours 5 minutes per day online, four in ten parents report finding it hard to control their child's screentime. Notably, 45% of 8-11s feel that their parents' screentime is too high, underlining the importance of modelling good behaviour.

Given the 13+ minimum age requirement on most social media platforms, it is notable that half (51%) of children under 13 use them. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third (36%) of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore will remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 25% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3- to 6-year-olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation

Annual Report) while considered to be safely using devices in the home and the 7–10-year-old age group remains the fastest growing for this form of child sexual abuse material.

Growing numbers of children and young people are using social media and apps such as Snapchat as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news. The alarming speed and scale at which misinformation about the attack in Southport (August 2024) was shared, resulting in Islamophobic and racist violence, rioting and looting across England is particularly concerning, with much of it was fuelled by false online accusations about the assailant. Despite attempts by Police and national news to correct the misleading information, it racked up millions of views on social media sites like X and was actively promoted by several high-profile users with large followings.

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2024 highlighting an increase in school attacks nationally, with 71% of secondary schools reporting a breach or attack in the past year, and 52% of primary schools.

Overview

Aims

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

- Setting out expectations for all King's C of E 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 filtering and monitoring through effective collaboration and communication with technical colleagues
- 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
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

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 Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and the Headteacher will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, LGFL 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 is shared 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 King's C of E Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, 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 and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, 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 there is one for All Staff which must be read even by those who have a named role in another section.

From September 2023, it is vital that all members of staff understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

The King's C of E Primary School has established a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, we also teach about online safety and harms through a whole school approach and provide an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

The King's C of E Primary School is committed to promoting the safe and responsible use of the internet, ensuring that all children are taught safe practice for use at school and at home. We currently use Education City, MyMaths and Google Classroom for online homework for all pupils. Other platforms used within the curriculum include Times Table Rockstars, Nessy and Reading Eggs. All organisations are committed to online safety and have published GDPR compliance for privacy and protection of data.

RSHE guidance also recommends that schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress."

Weekly computing lessons (taught through the Teach Computing scheme and Project Evolve) routinely address online safety, reminding children as appropriate to their age group, how to use use technology safely, respectfully and responsibly and how to keep themselves safe online.

Issues addressed include:

- Keeping personal information private
- Identifying where to go for help and support when they have concerns about content or inappropriate contact on the internet or other online technologies
- Age guidance for apps, games, DVDs, social media sites
- Using search engines safely and responsibly
- Following teacher/adult/parental guidelines for use and access
- Ensuring parental consent before using the internet at home
- Recognising acceptable/unacceptable behaviour online
- Identifying a range of ways to report concerns about content and contact (KS2)

In addition to the computing curriculum, termly Year Group/ Key Stage assemblies are used to present and address Online Safety issues, which are followed up and further explored in lessons.

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At The King's C of E Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

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 sharing this policy, sharing the curriculum, including relevant information in newsletters and resources on our website: Online Safety

Handling online-safety 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, PSHE/RSHE and Citizenship).

General concerns are 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 Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Cyber security risk assessment
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety, but recognises 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). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. The reporting member of staff will ensure that a record is made of the concern on CPOMS; this includes any concerns raised by the filtering and monitoring systems.

Any concern/allegation about staff misuse is always 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 the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 08000280285. This is displayed in the staff room.

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, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

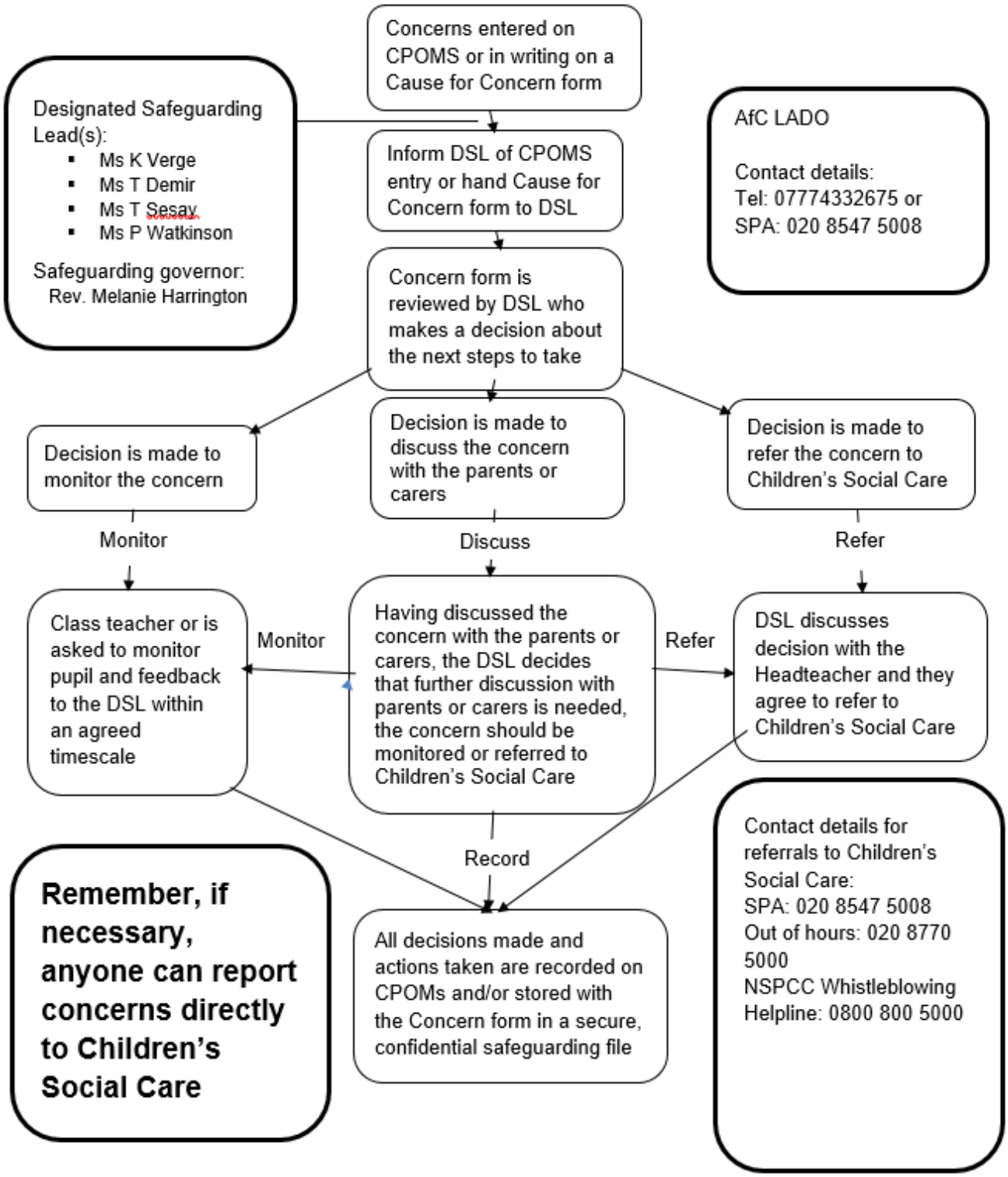
The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

If a problem comes to our attention that involves the safety or wellbeing of any of our pupils, The School has a duty of care to report under age profiles, inappropriate text messages and the use of inappropriate images to parents who will be informed and involved in any decision regarding their child's online activities.

In circumstances where there is a breach of online safety by any members of the whole school community then the 'What to do if' guidance from The London Grid for Learning (LGfl) will be followed (See appendix 8).

Please see below the flowchart for The King's C of E Primary School when raising concerns about a child. This can be found in the Safeguarding and Child Protection Policy.


Concerns entered on CPOMS or in writing on a Cause for Concern form
Designated Safeguarding Lead(s):
Ms K Verge
Ms T Demir
Ms T Sesay
Ms P Watkinson
Safeguarding governor:
Rev. Melanie Harrington
Inform DSL of CPOMS entry or hand Cause for Concern form to DSL
AfC LADO
Contact details:
Tel: 07774332675 or
SPA: 020 8547 5008
Concern form is reviewed by DSL who makes a decision about the next steps to take
Decision is made to monitor the concern
Decision is made to discuss the concern with the parents or carers
Decision is made to refer the concern to Children's Social Care
Monitor
Discuss
Refer
Class teacher or is asked to monitor pupil and feedback to the DSL within an agreed timescale
Monitor
Having discussed the concern with the parents or carers, the DSL decides that further discussion with parents or carers is needed, the concern should be monitored or referred to Children's Social Care
Refer
DSL discusses decision with the Headteacher and they agree to refer to Children's Social Care
Record
Remember, if necessary, anyone can report concerns directly to Children's Social Care
All decisions made and actions taken are recorded on CPOMs and/or stored with the Concern form in a secure, confidential safeguarding file
Contact details for referrals to Children's Social Care:
SPA: 020 8547 5008
Out of hours: 020 8770 5000
NSPCC Whistleblowing Helpline: 0800 800 5000

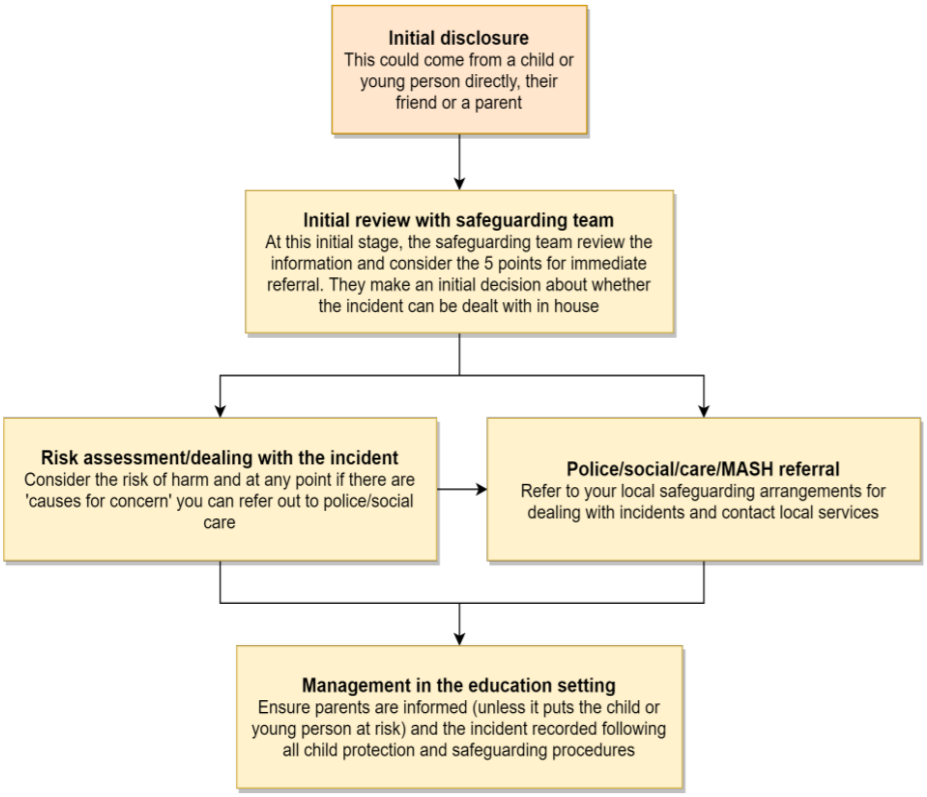
Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting. In the latest advice for schools and colleges (UKCIS, 2020), sexting is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

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) or online safety lead 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 to go straight to the DSL.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students 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 in turn 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.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

Upskirting

It is important that everyone understands that upskirting (taking a photo 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. Please refer to our Safeguarding and Child Protection Policy for more information around Upskirting.

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 anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. More information can be found on both our Anti-Bullying Policy and Safeguarding and Child Protection Policy.

The school takes bullying very seriously. **Any communication intended to offend, threaten, exclude or deride another person or their friends, family, gender, race, sexuality, culture, ability, disability, age or religion will not be tolerated and will be addressed in accordance with The King's School Anti-Bullying Policy.** Staff should be aware of trends of fights being filmed and fake profiles being used to bully children in the name of others.

Pupils are taught about bullying as part of the PSHCE curriculum, and online/cyberbullying is covered as part of this. **We expect all members of our community to communicate with each other with our school values of Love, Compassion and Respect, prominent at all times.**

Child-on-child sexual violence and sexual harassment

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.

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

The following procedures are in place 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 procedures are reinforced at the beginning of the school year but also pupils are reminded 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.

- All staff log in using allocated usernames and individual password. Pupils log on using their Google login.
- Pupils are taught how to save their work into their allocated place on their class Google Drive. This is essential for future access and for teacher monitoring of work.
- **We expect pupils to respect the contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission.**
- Pupil access to areas of the network, e.g. 'staffshare' is fully restricted.
- Pupils are taught to only print when necessary to save resources for financial and environmental reasons. **We expect pupils to only print out work when directed by staff to do so.**
- **We expect all users to make no attempt to alter the way the computer is set up.**
- Only the network administrators/teachers are permitted to install software on to computers. Pupils are taught that the network or an application may not function properly otherwise. Understanding this is key to avoiding future problems with home computing and internet activity.
- Any breaches of procedures and guidelines are followed up with through the behaviour policy.
- Increased focus on filtering and monitoring of the school's internet and systems will be shared with pupils, staff and parents via AUPs at the start of the academic year.

Monitoring software, provided by Senso, is installed on all the Chromebooks. This allows staff to closely monitor the pupils' use of the device. Alerts are given for misuse.

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/handbook.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the King's C of E Primary School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (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, the school will request that the post be deleted and will expect this to be actioned promptly.

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.

Home/ School Links

Part of The School's commitment to promoting safe and responsible use of the internet is to involve parents and carers, ensuring that children are supported at home to continue the safe practices learnt at school and in order that parents can make informed choices about use and monitoring.

In a time of ever-changing and developing technology, it is important that parents are involved and informed in order to support their children. The King's School provides the following support for parents:

- Shared acceptable use agreements
- Workshops on online safety
- Distribution of 'Digital Parenting Magazine'
- Information on resources and useful websites
- A web page on the School Website - About us – Safeguarding – Online safety
- Notification to parents of any concerns/issues
- Open door policy to discuss any concerns

The school encourages parents to discuss any concerns with class teachers and to be proactive in setting safe parameters for computing use at home following the acceptable use agreements.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will 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 widespread on certain platforms.

Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security 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. 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 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The Headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of USO-FX to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

The Headteacher/ designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with the School Business Manager and Click On It to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

The Headteacher, Web Filtering Governor and the school's IT technicians (Click On It) will work closely to ensure the above filtering and monitoring objectives are met and regular checks are carried out.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for children to bypass systems and any potential over-blocking. They can share any concerns with the DSL, in person and through CPOMS, and may be consulted for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum. We carry out half-termly checks to ensure all systems are in operation, functioning as expected and an annual review as part of an online safety audit of strategy and approach.

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

Our YouTube mode is 'strict restricted'. It can be turned to 'moderate restricted' when signing in to LGfL Authenticator.

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. Guidance and training regarding filtering, monitoring and the meaning of over-blocking can be found here: https://safefiltering.lgfl.net and safetraining.lgfl.net

There are three types of appropriate monitoring identified by the Safer Internet Centre and implemented by The King's C of E Primary School. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access

3. Active/Pro-active technology monitoring services

At The King's C of E Primary School:

- The internet connection and web filtering is provided by LGfL via SchoolProtect-WebScreen and Click On It. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. The school also uses Senso Cloud as an additional monitoring tool: Senso.cloud | Cloud-Based Device Monitoring and Management
- Changes can be made by Click On It
- Overall responsibility is held by the DSL with further SLT support from the Headteacher
- Technical support and advice, setup and configuration are from Click On It
- Regular checks are made half termly by the DSL, in consultation with the Web Filtering Governor to ensure filtering is still active and functioning everywhere. These are evidenced in the half-termly Headteacher reports to the Full Governing Board.
- An annual review is carried out in the Autumn Term-change if needed.
- Guidance on how the system is 'appropriate' is available at appropriate.lgfl.net
- According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:
- Physically monitoring by staff watching screens of users
- Network monitoring using log files of internet traffic and web access
- Individual device monitoring through software or third-party services

When using a school computer, Internet access is protected by filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is fully safe and we expect users to behave responsibly. Pupils are taught that the internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or damaging to the computer. **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.**

When accessing the internet through home computers or other computers out of school, we expect all pupils to maintain the same vigilance as taught in school. We also expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the internet.

The school website contains school policies, newsletters and other information. **We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers

electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

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

- Staff use the StaffMail system for all school emails

This is linked to the USO authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

Staff also use Microsoft Teams and Google to communicate and share files.

General principles for email use are as follows:

- Email and Google Classroom are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the Headteacher in advance. 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).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, the USO-FX system is available from LGfL.
    - Internally, staff should use the school network, including when working from home when remote access is available via the Freedon2Roam system.
- Appropriate behaviour is expected at all times, 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
- Pupils and staff are NOT allowed to use the email system for personal use 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.

Behaviour / usage principles of messaging/commenting systems

- More detail for all the points below are given in the **Error! Reference source not found.** section of this policy as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, 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 (including Teams and Google) 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

At The King's School, 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.

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 to the Senior Leadership Team. The site is managed by / hosted by e4education.

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that requirements are met.

Where other staff submit information for the website, they are asked to remember:

- 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. If in doubt, check with the Headteacher or School Business Manager. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our Data Protection policy. The cloud platforms we use are Microsoft's Office 365, Google Classroom and Microsoft Teams.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager manage the pupil's passwords, analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

Digital still and video cameras are used for recording special events as well as being important tools for everyday learning experiences across the curriculum.

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:

- I am happy for the school to **take** photographs of my child.
- I am happy for photos to be **used** on the school premises i.e. on displays, to showcase work, recording an event, supporting the curriculum.
- I am happy for photographs to be **used** on school publications i.e. PowerPoint presentations which could be shown to other parents, schools or educators, website, newsletters, as evidence of learning in other children's exercise books.
- I am happy for photos that include my child to be **shown** and/or sold to others (we only sell to families and guardians), example of such include class photographs, Year 6 yearbook.
- I am happy got photos to be **shared** with the local newspaper.

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.

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).

Some images celebrating pupils' work, as well as every day and special event activities, may be selected to be shown on the school website. A child's full name will never be used alongside their image. **The school will remove any image of a child on the school website at their parent's request.**

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 The King's C of E Primary School, members of staff may occasionally use personal phones to capture photos or videos of pupils in school, on school trips or sports events.

However, 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 or cloud services (NB – many phones automatically back up photos). Staff must therefore proactively turn off cloud sharing and should refer to the manufacturer's or third-party supplier's instructions. If staff are unsure how to do this then they must ask the School Business Manager/ CITL.

Photos are stored on the school network and under no circumstances should a child's name be used as part of or as the filename for an image. It is the individual staff member's responsibility to follow these guidelines, in line with the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (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 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

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

The King's C of E Primary School's SM presence

The King's C of E Primary 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.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

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, even if there are no official/active school social media accounts."

Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) 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 which all members of the school community sign, 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 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 (including Instagram, Facebook and Snapchat) have a minimum age of 13 (note that WhatsApp is 16). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other 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 (you don't need to know them – ask your child to explain it to you), 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 Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Email and Google Classroom are the official electronic communication channels between parents and the school, and between staff and pupils.

Pupils/students 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/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). 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 student 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.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 6 years, there have been 333 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

The use of social networking and online media

The King's School asks its whole community to promote the 'three commons' approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory, or encourage extremist views. This is online bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. Creating or forwarding such materials can make us liable for prosecution.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

If any member of staff, student or parent/ carer is found to be posting libelous or inflammatory comments on the internet or any social media, they will be reported to the appropriate 'report abuse' section of the network site (all social media have clear rules about content which can be posted and have robust mechanisms to report breaches). Pupils and staff would be sanctioned appropriately, and we expect parents to support us in this and behave appropriately themselves.

In serious cases, we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting inappropriate sexual approaches towards children at **thinkuknow.co.uk/parent**

Device usage

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 acceptable use policies and the following sections of this document which all impact upon device usage: 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/students:** Pupils are not permitted to have mobile phones in the classroom. We understand that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security

grounds as they are easily lost, damaged or stolen. Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day. **We expect pupils not to carry a mobile phone in school or on any school trip/residential journey.**

- **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. See also the Digital images and video section on page and Data protection and data security section in this policy. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** 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) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document in this policy. (check staff handbook)

Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **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.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal All internet traffic is monitored.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Electrical Safety and Care

Electrical equipment in the school is tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHCE curriculum.

- We expect pupils to behave appropriately near electrical sockets and appliances.
- Plug sockets are fitted with protector covers where appropriate.
- No food or drink is permitted near computers.

- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks.
- We expect all users to take responsibility for their own physical well-being by adopting good practices.
- Computers and other IT equipment can be easily damaged. Pupils are taught the correct way to use IT equipment, switching on and off, getting out and putting away laptops for recharging, and attaching devices such as headphones and electronic microscopes. Pupils are taught to walk and never run when moving equipment from one place to another in the school.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher/Principal 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 1 – Roles

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

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the "All Staff" section.

Roles:

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

All staff

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the

school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Headteacher – Ms K Verge

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 Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- 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
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how.
- 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
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process
- 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 GDPR-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 needs of pupils, including risk of children being radicalised
- Have an understanding and review, along with the school's IT technicians, the DSL and Web Filtering Governor, the school's systems for filtering and monitoring use of the school's internet and the devices that are using it. This understanding also includes knowing what is blocked or allowed for whom, when, and how as per KCSIE. KCSIE Web-filtering | LGFL

- In consultation with the DSL, the school's IT technicians and the Web Filtering Governor, undertake regular filtering and monitoring checks of the school's internet usage and report to the Governing Board. LGfL's Safeguarding Shorts: Filtering for DSLs and SLT
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Ms K Verge & Ms T Demir

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

- "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] … this **lead** responsibility should not be delegated"
- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Take lead responsibility for webfiltering and monitoring of the school's internet usage and systems
- Have an understanding and review, along with the school's IT technicians, the Headteacher and Web Filtering Governor, the school's systems for filtering and monitoring use of the school's internet and the devices that are using it. This understanding also includes knowing what is blocked or allowed for whom, when, and how as per KCSIE. KCSIE Webfiltering | LGFL
- In consultation with the Headteacher, IT technicians and the Web Filtering Governor, undertake regular filtering and monitoring checks of the school's internet usage and report to the Governing Board. In doing so, review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping LGfL's Safeguarding Shorts: Filtering for DSLs and SLT
- Ensure ALL staff undergo safeguarding and child protection training (including online safety, which incorporates filtering and monitoring guidance) at induction and that this is regularly updated
- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees 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 online safety 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 (spotlight)

- 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 GDPR-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 and "undertake Prevent awareness training."
- 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/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- 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 an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee 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 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/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE "be careful that 'over blocking' does not lead to unreasonable restrictions".
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that 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).
- Facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net
    - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
    - cascade knowledge of risks and opportunities throughout the organisation

- cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents.

Governing Body, led by Online Safety / Safeguarding Link Governor – Rev Melanie Harrington

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 and Trustees 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. Free Governor safeguarding training: safetraining.lgfl.net
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Appoint a Web Filtering Governor to work closely with the DSL on filtering and monitoring standards at the school. Guidance can be sought from: safefiltering.lgfl.net
- Have regular strategic reviews, incorporating discussions about filtering, monitoring and blocking, with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Headteacher to ensure a GDPR-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
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net

- "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 / RSHE Lead/s – Ms M Huggins

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-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." Training is available at safetraining.lgfl.net
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to 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"
- This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included 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 – Ms S Carter

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 an 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 new 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/technician (SBM) – Mr A Rooney

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. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- Support DSLs and SLT to carry out an annual online safety audit as now 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), protections for pupils in the home and remote-learning. LGfL has a free template you can use at https://onlinesafetyaudit.lgfl.net
- Keep up to date with the school's online safety policy and technical information in order 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 of any changes to these systems (especially in terms of 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.
- 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 that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare. These solutions which are part of your package will help protect the network and users on it
- Monitor the use of school technology, online platforms and social media presence and 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) – Mr A Rooney (SBM)

Key responsibilities:

- NB – this document is not for general data-protection guidance; GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there is an LGfL document on the general role and responsibilities of a DPO in the 'Resources for Schools' section of that page
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2, 18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.

- Work with the DSL, Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL schools for three market-leading GDPR compliance solutions at gdpr.lgfl.net
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

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 / online safety coordinator as named in the AUP
- 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 and review this annually
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's 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.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at

parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

External groups, including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within 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 other's 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

Appendix 2 – Related Policies and Documents

1. Safeguarding and Child Protection Policy
2. Behaviour Policy
3. Anti-Bullying Policy
4. Staff Code of Conduct / Handbook
5. Acceptable Use Policies (AUPs) for:
    - Pupils
    - Staff, Volunteers Governors & Contractors
    - Parents
6. Letter to parents about filming/photographing/streaming school events
7. Online-Safety Questions from the Governing Board (UKCIS)
8. Education for a Connected World cross-curricular digital resilience framework (UKCIS)
9. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
10. Working together to safeguard children (DfE)
11. Searching, screening and confiscation advice (DfE)
12. Sharing nudes and semi-nudes guidance from UKCIS:
    - *How to respond to an incident - overview for all staff
    - *Full guidance for school DSLs
    - *Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
13. Prevent Duty Guidance for Schools (DfE and Home Office documents)
14. Data protection policy
15. Cyber Security Risk Assessment
16. Cyber bullying: advice for Headteachers and school staff (DfE) – find this at bullying.lgfl.net
17. LGFL Links for Online Safety
18. RAG (red-amber-green) audits for statutory requirements of school websites
19. Ofsted Review of sexual abuse in schools and colleges

Appendix 3 – Acceptable Use Agreement: EYFS

S

I will only use tablets, computers, electronic devices, internet sites and apps that I am allowed to use. I will ask for help if I am stuck or not sure and will tell a trusted adult if I am worried, upset, scared or confused about anything I see online.

A

I know that people on the internet are not always who they say they are and not everything I read or see on the internet is true. I will look out for my friends and tell someone if they need help.

F

I will only send friendly and polite messages to people and treat them the way I would like to be treated myself. I know that anything I do online can be shared and might stay online forever.

E

I will not keep secrets or follow dares, challenges and instructions from someone I do not know. I will not change my clothes or get undressed in front of a camera. I always check before sharing my personal information or other people's stories and photos.

My name: _____

Appendix 4 – Acceptable Use Agreement: KS1

My name is _____

This is how I keep **SAFE online:**	✓
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

Appendix 5 – Acceptable Use Agreement: KS2

These statements can keep me and others safe and happy at school and home:

1. ***I learn online*** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – As well as looking at things from other people on apps, sites and games, I also get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
11. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
12. ***I know new online friends might not be who they say they are*** – 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.
13. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
14. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
15. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
16. ***I 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 should say no, stop chatting and tell a trusted adult immediately.
17. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
18. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.

19. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
20. ***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).
21. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school that includes _____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed: _____ **Date: _____**

Appendix 6 – Acceptable Use Agreement: Staff, Governors, Volunteers, Students, Peripatetic teachers, Club leaders, Contractors

What is an AUP?

We ask all children, young people and adults involved in the life of The King's C of E Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read The King's C of E Primary School's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc.

If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher.

What am I agreeing to?

1. I have read and understood The King's C of E Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
3. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
4. I will take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment - and maintain an attitude of 'it could happen here'
5. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language

6. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.
7. During remote learning:
    - I will not behave any differently towards students compared to when I am in school. I 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.
    - I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
    - I will not take secret recordings or screenshots of myself or pupils during live lessons.
    - I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    - I will log and report any issues for live lessons immediately to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult). If anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students.
8. I understand that in any periods of home learning, school closures or potential lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
9. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
10. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
11. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.
12. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and will first seek guidance from the DSL.
13. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and our Online Safety Policy.
14. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change

passwords and notify the Headteacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

15. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
16. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
17. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
18. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
19. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Staff can either sign below or digitally sign using the Google Form.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Online Safety Lead

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems (S Drive, Google Classroom, Teams, LGFL):

_____

Additional permissions (e.g. admin):

_____

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 7 – Acceptable Use Agreement: Parents/ Carers

Background

We ask all children, young people and adults involved in the life of The King's C of E Primary School to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP.

We tell your children that **they should not behave any differently when they are out of school or using their own device or home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read the school's full Online Safety Policy on our website (www.kings.richmond.sch.uk) for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher.

What am I agreeing to?

1. I understand that The King's C of E primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, including during any remote learning periods.
4. **I understand that my child might be contacted online via Google Classroom and only about their learning, wellbeing or behaviour. If they are contacted by someone else or these staff ask them to use a different app to chat, they will tell another teacher.**
5. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's 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.
6. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

7. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
8. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...
9. I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
10. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
11. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
12. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
13. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
14. I can find out more about online safety at The King's C of E Primary School by reading the full Online Safety Policy on our website (www.kings.richmond.sch.uk) and can talk to my child's class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

Please note that parents may also be interested in the school's approach to the following matters, which are all covered as sections within the overall school Online Safety Policy:

- Roles and responsibilities of members of the school community
- Education and curriculum
- Handling online-safety concerns and incidents
- Actions where there are concerns about a child
    - Sexting and upskirting
    - Bullying
    - Sexual violence and harassment
    - Misuse of school technology (devices, systems, networks or platforms)
    - Social media incidents
- Data protection and data security
- Appropriate filtering and monitoring
- Electronic communications
- Email
- School website
- Cloud platforms
- Digital images and video
- Social media
- Device usage

Appendix 8 – Use of digital images and video permission (Parents/ carers)

To comply with the General Data Protection Regulation (which supersedes the 1998 Data Protection Act), we need your permission before we can photograph or make recordings of your daughter / son.

The King's School rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Any photos /videos taken by staff are downloaded to the approved school site immediately and deleted from their personal device.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made by a child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators, e.g. in our school prospectus or on our school website. On rare occasions, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if they won a national competition and wanted to be named in local or government literature.

Appendix 9 – The King's School Guide – What to do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/online safety coordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: **Atomwide via the LGFL Helpdesk**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.
6. In an extreme case where the material is of an illegal nature:
    a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (undertaken by Headteacher).
    - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
    - Contact the local police and follow their advice.
    - If requested to remove the device to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online-safety anti-bullying and PHSCE and apply appropriate sanctions.

3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, LGFL)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc.).
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child.

1. Report to and discuss with the named DSL in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.

1. Report to and discuss with the named DSL in school and contact parents.
2. Advise the child and parents on appropriate games and content (you may want to use LGFL template letters to inform all or targeted parents).
3. If the game is played in the school environment, ensure the technical team block access to it
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training to discuss how to behave/appropriate responses to such posts
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and online-safety officer. **Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.**

Appendix 10 – The King's School – Password Procedure

Within The King's School, each electronic system that is accessed is password protected. This password may be set by the school or by the third-party provider of the system. Staff should not share usernames and passwords and under no circumstances should they be divulged to pupils. If at any time a member of staff thinks that their access to any of the system has been compromised they should inform their line manager or contact the IT technician. There are school wide systems which are detailed below.

School Network:
Usernames and Passwords are set by the school and the Password is required to be reset on first use. Passwords can be reset by staff at any time.

LGFL (London Grid for Learning) StaffMail (school email) and Services
Usernames and passwords are issued by LGFL and passwords can be reset by individual users.

Arbor:
Usernames and Passwords are set by the school and passwords are required to be changed every 90 days.

Google Accounts (access to the King's School Google domain only):
Usernames and Passwords are set by the school and passwords can be reset by individual users.

My Maths
Usernames and Passwords are set by My Maths but can be managed and reset by the school.

Education City:
Access is controlled by a network setting and no username or password should be required

All other systems:
Staff may access other systems from within school (e.g. Twinkle, TES) but the school has no control or responsibility for access to these systems.

Appendix 11 – Useful Links

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
Disrespect Nobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
SWGfL	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
Parent Zone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
PSHE Association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
Educate Against Hate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	advice for schools and colleges
net-aware	NSPCC advice for parents
Common Sense Media	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching Screening and Confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGfL	Advice and resources from the London Grid for Learning

Appendix 12 – Acceptable Use Agreement SEND

(Attached Separately)