Ridgeway Primary School and Nursery

Online Safety Policy

Status:	Statutory
Source:	LGfL Template Policy (Cross-referenced with existing school policies)
Last reviewed by:	HST
Approved by:	HST & Safeguarding governor
Date of approval:	29/1/2026
Frequency of review:	Annually
Date for next review:	Autumn 2026
Published on:	School Website / Weduc

Policy is written in conjunction with: Safeguarding Policy; Data Protection Policy; Cyber Security Policy

Revision date	Section:	Significant changes made:
21/12/2019		New policy
18/1/2022		Multiple revisions throughout
8/11/2022		Minor revisions throughout (mostly to reflect updates from KCSIE 2022 and other government documentation referenced in the policy)
22/9/2023		Multiple revisions throughout – policy adapted for Ridgeway from the LGfL template (which encompasses changes in KCSIE 2023)
12/12/2025		Multiple revisions throughout – policy adapted for Ridgeway from the LGfL template (which encompasses changes in KCSIE 2025). Key changes to note: Introduction of a 'Use of Generative AI' section

Introduction

Key people / dates

	Headship Team (HST)	Suzanne Kelly (Co-Head and IT lead) Rebecca Shelley (Co-Head) Jonathan Smith (Deputy Head) Kayley Dunn (Assistant Headteacher)
	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Kayley Dunn
	Deputy Designated Safeguarding Leads / DSL Team Members	Rebecca Shelley Suzanne Kelly (Filtering & Monitoring Lead) Jonathan Smith (Online Safety Lead) Sarah Jackson (SENCo) Chris Avery (Nurture Lead) Charlotte Robinson (Nurture Support) Dan Leahy (Acorns Manager)
	Link governor for safeguarding	Suzannah Flanagan
	Curriculum leads with relevance to online safeguarding and their role	Jonathan Smith (School curriculum lead) April Williams (Computing curriculum lead) El Jeffrey (Wellbeing curriculum lead)
	Network Manager / IT Technician	Geoff Blyth (Network Manager - Curriculum) Jack Clancey (IT Technician - Curriculum) Croydon Education Partnership IT (Admin network management/support)
	Date this policy was reviewed and by whom	December 2024 - Jonathan Smith
	Date of next review and by whom	Ongoing updates as required. Full review due September 2026 by Jonathan Smith

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy 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. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see safepolicies.lgfl.net) for different stakeholders help with this. Any changes to this policy will 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 and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads (e.g. for RSHE) will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What were the main online safety risks in 2024/2025?

Current Online Safeguarding Trends At Ridgeway

In our school in recent years, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

	Solutions to mitigate the risks
Identified Risky Behaviours	**At Home**
Children having unrestricted access to the online world, especially: YouTube, social media and online gaming	Find out about ways to restrict children's online access, including the use of safety settings on devices. Talk to children about what they want to access and why and ensure it is age appropriate and does not put them at risk of inappropriate content being accidentally viewed. View content with or before your child, to ensure it is appropriate. (Note that many social media and digital platforms use algorithms to drive content towards the end user and these can lead to undesirable suggestions being shown.)
Children accessing the online world without any/adequate supervision: many children, especially in KS2 but increasingly across all age groups, report using devices online without an	Ensure children are supervised at all times when online and discuss with them what it is they do/access when online – part of the children's learning we teach in school is about always telling the adults at home what you are doing when online, so talk to them about this and set your own expectations at home.

adult present, especially in their own bedrooms while on their own	
Children accessing inappropriate online content, especially: age inappropriate video clips (especially horror or scary clips), music with inappropriate content (especially explicit language and/or sexualised behaviours), age inappropriate online gaming, age inappropriate language (especially swearing), sexually inappropriate language and video content	If suitable restrictions and supervision are in place, this considerably mitigates this risk, but it is also worth having conversations with your children about what content is appropriate/inappropriate and what to do if they encounter something that is inappropriate, makes them feel worried or unsafe – children share that the main reason for not informing adults at home what they do online, is fear of having devices taken away, so open, honest dialogue and developing a shared understanding of what is appropriate or not is vital
Children posting messages and/or photos and/or videos of themselves online	School would encourage children to not post online content, especially photos and videos of themselves. However, we recognise that children are increasingly interested in this area. We encourage families to discuss with their child whether posting online is appropriate and desirable in the first place. If so, ensure any platform/forum used is age appropriate and ensure any privacy settings are enabled to ensure content is only shared with known and trusted contacts. Discuss the fact that once content is posted it can be used by others in ways they did not originally intend and/or others might comment on their content in ways they might not like.
Children communicating with strangers online	Ensure you know what systems/games children use to communicate with others and only let them do so with people they actually know and trust (i.e. have met in the physical world)
Children joining online groups (often through gaming) that include strangers	
Children sending one another abusive messages through social media/online message forums (i.e. cyber bullying)	Discuss with children: how to behave; how inappropriate behaviours would make them/others feel; and online reputations and how things that are posted online can be seen by many and potentially forever.

At Ridgeway Primary School, in addition to what we do to mitigate these individual risks, we also do the following:

- Treat each and every online safety incident as a Safeguarding issue and record and manage the response in line with our safeguarding policy. Staff use any incidents as an opportunity to talk to children and understand how and why situations have arisen. We then support and educate children, as well as families, about how to behave safely and appropriately when online.
- Cover the full range of online safety learning through both our Wellbeing and Computing curricula, to ensure full and thorough coverage. Year groups will cover online safety in the following ways, throughout the year:
    1. **Teach -** Cover an element of the online safety curriculum every half term
    2. **Follow up –** The HST will cover online safety for Years 1-6 in assemblies at different points during the year. Teachers will have follow up conversations in class with children to reinforce this learning
    3. **Reinforce –** Throughout the year when teaching other subject content, staff will **actively seek opportunities for reinforcing online safety learning** that is relevant (e.g. when researching online, make explicit links to managing information online and differentiating between

opinion, belief and facts; or when looking at relationships and communicating with other, discussing the relevance of this in both the physical and online worlds)

4. **Respond –** As part of their everyday roles, staff monitor children's behaviours and conversations to look for signs of anything concerning or inappropriate. If an online incident occurs, or staff notice some unhealthy or concerning online behaviours or attitudes, these are used as a learning opportunity to help remind/teach children about the relevant online safety topic (e.g. A conversation comes up about sharing passwords)

Current Online Safeguarding Trends Nationally

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.

Last year, we highlighted the rapid rise of generative AI (GenAI). Since then, the trend has exploded. Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many students can access freely at home or school. Chatbots can also blur reality, offering harmful advice or engaging in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.

When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.

Beyond text, GenAI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery. Alarming reports also show children using nudifying apps to create illegal content of peers.

We regularly see AI searches involving sexualised and harmful content. It's critical to stress that in the UK, *any* CSAM (child sexual abuse material)—AI-generated, photographic, or even cartoon—is illegal to create, possess, or share.

Ofcom's 'Children and parents: media use and attitudes report 2025' has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram. With children aged 8-14 spending an average of 2 hours 59 minutes a day online across smartphone, tablet and computer – with girls spending more time online than boys, four in ten parents continue to report finding it hard to control their child's screentime. Notably, 52% of 8-11s feel that their parents' screentime is also too high, underlining the importance of modelling good behaviour.

Given the 13yrs+ minimum age requirement on most social media platforms, it is notable that over half of 3-12-year olds (55%) were reported using at least one app. 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 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.

We have also come across online communications platforms that offer anonymous chat services and connect users with random strangers allowing text and video chats. Most of these are easily accessible to children on devices.

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 for the first time, there were more 7-10-year-olds visible in child sexual abuse material (CSAM) images than 11-13s.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news. There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm. See nofilming.lgfl.net to find out more.

Cyber Security is an essential component in safeguarding children and features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2025 reporting high levels of schools being attacked nationally, with 60% of secondary schools and 44% of primary schools reporting a breach or attack in the past year.

How will this policy be communicated?

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

- Posted on the school website in the Key Information / Online Safety section
- Available in paper format in the staffroom

Contents

Overview

Aims

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

- Setting out expectations for all Ridgeway Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.

- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

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

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning 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 A 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. There are also pupil, governor, etc. role descriptions in the appendix. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

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

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and 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, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

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

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

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE) – At Ridgeway this is encompassed within our Wellbeing curriculum
- Computing

- Citizenship

However, as stated previously, 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.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Ridgeway Primary School, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum. Online safety will be a key element of our Wellbeing curriculum. We will use sources (such as the cross-curricular framework 'Education for a Connected World' from UKCIS) when planning our coverage of online safety.

Annual reviews of curriculum plans (including for SEND children) 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. Details of our online safety learning intent can be found in the Wellbeing and Computing curricula in the Online Safety section of our school website: Online Safety - Ridgeway Primary School & Nursery. This is done within the context of an annual online safety audit, which is a collaborative effort led by the school's curriculum lead.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) 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.

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
- Cyber Security Policy
- Behaviour Policy (including Anti-Bullying Policy)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use, etc.)
- Staff Discipline & Conduct Policy

This school commits to take all reasonable precautions to safeguard pupils online 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 the school's safeguarding record system – CPOMS. This includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

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

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.
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 concerning or breaks the law.

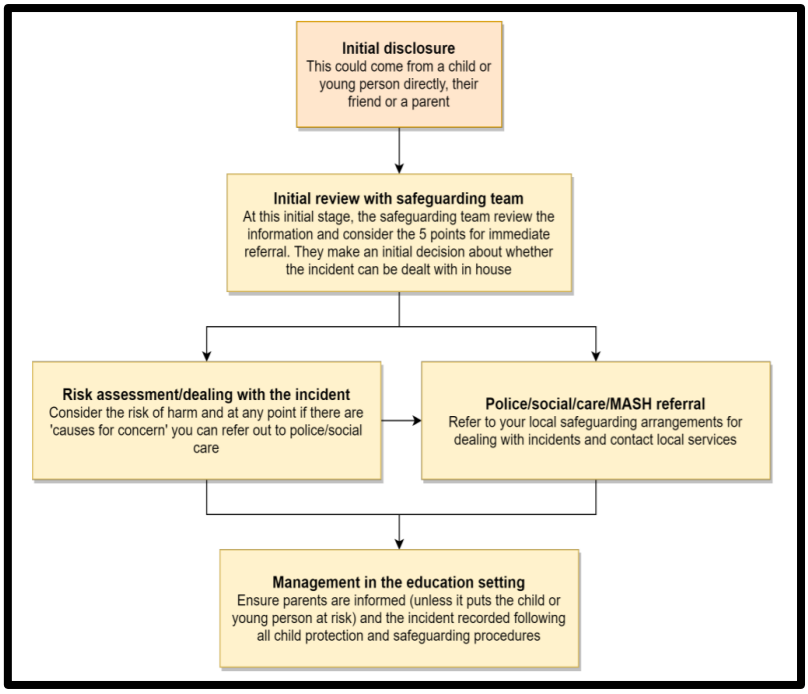
Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

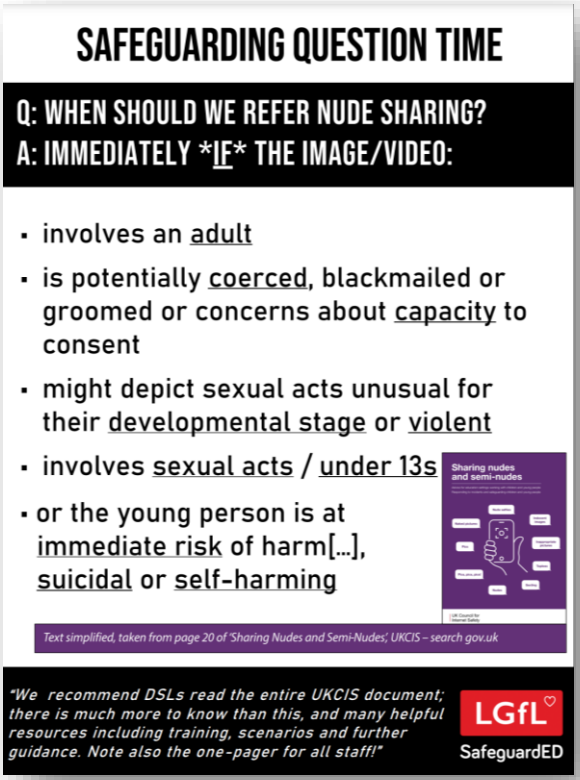
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of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

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 use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.



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



Priority Areas

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in

Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

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

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 guidance in KCSIE. 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. This will be discussed in staff training.

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

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

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

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.

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

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

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies and online safety policy.

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Ridgeway community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school Behaviour Policy (for children and families) or Staff Discipline and Conduct Policy (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, Ridgeway 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.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty, which is contained within our safeguarding policy which can be found here. 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 cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy which can be found here. 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 2025, "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."

Appropriate filtering and monitoring

A designated safeguarding lead (DSL - Filtering & Monitoring Lead) has lead responsibility for filtering and monitoring and works closely with the school's Network Manager and IT Technician 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.

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

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via and will be asked for feedback at the time of the regular checks which will now take place. They can submit concerns at any point and will be asked for feedback at the time of the regular checks which will now take place. Staff submitting concerns email the IT Technician with the subject header **'Filtering and Security Concern'**, unless the concern poses an immediate safeguarding risk in which case they should immediately report to a DSL as per the safeguarding policy. All concerns are logged and follow-up actions are recorded by the school's Network Manager or IT Technician. This log is also monitored by the DSL (Filtering & Monitoring Lead).

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 monitor on an on-going basis with termly checks to ensure filtering is operational, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

At our school we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. We apply the LGfL filtering that includes Chat GPT, Gemini, Co-Pilot and Claude. This group has been allowed for Teachers and Admin Staff only, and not for children. If we decide to include AI within our curriculum for children, we will do so in line with DfE guidelines.

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

We recommend the use of 'Kidrex' and 'Kiddle' for younger children on our Curriculum Network.

We do not allow children to access YouTube themselves. Teaching Staff can access YouTube in 'Restricted Mode' by authenticating their credentials when required. This helps us to limit inappropriate content that is served to pupils.

Out of hours, our policies are:

- Filtering Reports are not scheduled to run 'Out of Hours'. However, if there has been cause for concern, Nominated Contacts may choose to run an ad-hoc report at any time.
- Curriculum Network machines are set to shut-down for out of hours periods as an energy saving feature. However, Sophos runs on any active equipment with emails sent to Network Managers.

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.

The DSL (Filtering & Monitoring Lead) checks filtering reports and notifications on a half-termly basis and, in collaboration with the Network Manager and/or IT Technician, takes any necessary action as a result.

According to the DfE standards, "Your monitoring plan should include how you will monitor students when using school-managed devices connected to the internet. This could include:

- device monitoring using device management software
- in-person monitoring in the classroom
- network monitoring using log files of internet traffic and web access"

At Ridgeway:

- web filtering is provided by LGfL using the WebScreen3 system on school site. Any school devices provided for home use will also be installed with an appropriate web filter
- changes to the local filtering can be made by the school's Network manager/IT Technician
- overall responsibility is held by the DSL (Filtering & Monitoring Lead), with support from the HST and Computing Lead
- technical support and advice, setup and configuration are from LGfL or the school's Network Manager/IT Technician
- regular checks are made at least half termly by the Network Manager/IT Technician to ensure filtering is still active and functioning everywhere. These are evidenced on the filtering and monitoring check-list and discussed with the DSL (Filtering & Monitoring Lead)/DSL Safeguarding Team
- an annual review is carried out as part of the online safety audit to ensure a whole school approach
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

At Ridgeway, we use a combination of all three types of monitoring to keep children safe:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access monitoring
3. Active/Pro-active technology monitoring services

Sophos Endpoint solution runs on any active equipment and reports to 'Sophos Central' dashboard. Network Managers are then alerted by email for action as appropriate.

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

Authorised systems

- Children do not currently use email within school.
- Staff and governors at this school use the LGfL StaffMail system for all school emails. They do not use their school email to communicate with children or families.
- Staff (generally only the office staff and HST) at this school use Weduc to communicate with families.

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

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed in line with school policies.

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 Co-Headteacher (if by a staff member).

If this a private account is used for communication or to store data by mistake, the Co-Headteachers should be informed immediately.

Behaviour / usage principles of messaging/commenting systems

General principles for email use are as follows:

- Email and Weduc are the only means of electronic communication to be used between staff and children / staff and families (in both directions). Use of a different platform must be approved in advance by the Co-headteachers. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the HST (if by a child) or to the DSL or a DSO (if by a staff member)
- Email may only be sent using the school email system or via Weduc. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Co-headteachers/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately
- Staff or children's personal data should never be sent/shared/stored on email:
    - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL
    - Internally, staff should use the school network or MyUSO (LGfL's secure cloud storage facility), including when working from home. On the school's Admin network (used by the school office and HST) remote access is available via the Home 2 Office Remote Access system provided by Octavo Partnership
- If email were used by children (using the system described above), children in all year groups will be restricted to emailing within the school and cannot email external accounts
- Appropriate behaviour is expected at all times, on all systems/communication channels, 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

- Children 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
- 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 and governors should not use the email system for personal use.

Use of generative AI

At Ridgeway Primary School, we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini 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. This will be through assemblies, in class learning, through family meetings and the weekly Newsline. 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, nudifying apps and inappropriate chatbots).
- 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.
- In school, we do not allow children access to generative AI tools.
- If staff require access to 'AI Tools' they have to authenticate themselves at the 'Block Page' with their USO Credentials. They are not permitted to submit any personal data about colleagues or children when using AI tools.
- Security on the Curriculum Network prevents staff from directly installing new platforms. Any New platforms would go for approval with the HST and Computing Lead in conjunction with the Network Manager.
- AI is not currently part of the school's curriculum offer. If this changes, we would discuss and carefully plan the parameters around its introduction and use by children.

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.
For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Ridgeway has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times. These can be found in the policies section on Weduc.

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 children safe, and to avoid incidents. The OSL and Network Manager analyse and decide on which systems and procedures to use before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform families when and what sort of data is stored in the cloud
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that children's data is not shared by mistake. Open access or widely shared folders are clearly marked as such

- Children 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 administrative access to staff or children's data
- Children's images/videos are only made public with parental permission
- Only school-approved platforms are used by children or staff to store children's 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)

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 Co-Headteachers and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the school's office staff. The DfE has determined information which must be available on a school website and school reviews the requirements regularly, but at least on an annual basis to ensure compliance.

The site is managed by / hosted by FSE Design.

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

- School has the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public domain images that can be used. Children and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where children's work, images or videos are published on the website, their identities are protected and full names are not published (including not saving images with a filename that includes a child's full name)

Digital images and video

When a child joins the school, families/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). Families are able to amend their permissions and decline consent at any time and must do so in writing. Families provide permission for the following:

- Name to be used on the school website, publications and local media
- Learning in which they can be identified (e.g. by their name) to be used in school displays
- Learning in which they can be identified (e.g. by their name) to be used on the school intranet (e.g. secure systems only school staff and families can access)
- Learning in which they can be identified (e.g. by their name) to be used on the school website
- Image to be used in books, folders and/or learning journals as evidence of learning
- Image to be used within the school building (for example, in wall-mounted displays and on display screens)
- Image to be used on school intranet (e.g. secure systems only school staff and families can access)
- Image to be used in school publications (for example, Newsline, school brochures)
- Image to be used on the school website
- Image to be used on social media by organisations with whom school works in partnership (e.g. community groups)
- Image to be used in the local media
- Image to be taken by the school photographer for individual and sibling photos. (We will not be able to include your child in these photographs if consent is **not** given)

- Image to be taken by the school photographer for whole class photos (We will not be able to include your child in these photographs if consent is **not** given)

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

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

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

Photos are stored on the school network in line with the Document Retention Policy.

Families/carers can be given permission by a member of the HST to take photographs or videos at specific events. Families/carers are reminded about the importance of not sharing photographs or videos via any form of media (including social media) due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection).

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

Children 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, families or younger children.

Children 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 personal information public.

Children 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 / a friend are subject to bullying or abuse.

Social media

Our SM presence

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school 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 monitor our social media footprint carefully to know what is being said about the school and track and respond to individuals in a fair, responsible manner, even though there are no official/active school social media accounts.

Staff, pupils' and parents' SM presence

Social media (including 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 families, staff and children 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. family chats, pages or groups.

If families 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 policy should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, children and families, also undermining staff morale and the reputation of the school (which is important for the children we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving children under the age of 13. We ask families 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 children/children 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.

Families 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 Digital Family Agreement to help establish shared expectations and 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/or Weduc are the official electronic communication channels between families and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

The school uses Weduc as a learning platform. It should only be used for matters related to learning.

Children 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.

Children and families should not 'follow' 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; this highlights the need for staff to remain professional in their private lives and use of social media. In the reverse situation, however, staff must not follow such public child accounts.

* Exceptions may be made (e.g. for pre-existing family links), but these must be approved by the Co-headteachers, and should be declared upon entry of the child 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 staff member) or to the Co-headteachers (if by a child).

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 or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

We 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)

- **Children** in KS2 are allowed to bring mobile phones in to school, with parental permission, if deemed necessary (for example if they are walking home by themselves). Children must hand in their mobile phones to their class teacher as soon as they arrive at school. Mobile phones must be switched off before being handed in. Children may have this privilege withdrawn if they do not adhere to these rules. In the case of emergencies, important messages and phone calls to or from families will be made via the school office. Children must not use any personal device (including mobile phones, cameras, watches, etc.) to take photographs or video recording anywhere on the school site.
- **All staff who work directly with children** should leave their mobile phones on silent or switched off and ensure they are stored in a cupboard or bag (i.e. not in a pocket) during learning time and when staff are in learning spaces (e.g. classrooms and corridors). Staff should only use their mobile phones during break times and in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.
- **During periods of remote learning**, it might be necessary for staff working from home to use a personal device to contact a family. They will only do so for official school business and will ensure their private number is blocked when doing so.
- **Volunteers, contractors, governors** should leave their phones in their pocket/bag and turned off when they are **on site**. 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 Co-headteachers should be sought (the Co-headteachers may choose to delegate this authority) and this should only be done in the presence of a member of staff.

- **Families** are asked to leave their phones in their pockets/bag and turned off when they are **on site**. Permission to take photographs and/or videos may only be given by the HST. Any and all photographs and/or videos are for personal viewing only and must not be shared via any method (text, email, social media, etc.)

Use of school devices

Staff and children are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home. School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct. Wifi is available on request to school staff and governors for school-related internet use and limited personal use within the framework of the acceptable use policy. All such use is monitored. School devices for staff or children are restricted to the apps/software installed by the school, whether for use at home or school, and may only be used for learning. All and any usage of devices and/or systems and platforms may be tracked.

- **Children** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network, using school equipment (e.g. laptops/tablets) for school-related internet use within the framework of the Acceptable Use Policy. All such use is monitored
- **Staff** can access the guest wireless network, subject to the Acceptable Use Policy, but have no access to networked files/drives. All internet traffic is monitored.
- **Volunteers, contractors** can access the guest wireless network, subject to the Acceptable Use Policy, but have no access to networked files/drives. All internet traffic is monitored.
- **Governors** can access the guest wireless network, subject to the Acceptable Use Policy, but have no access to networked files/drives. All internet traffic is monitored.
- **Families** have no access to the school network or wireless internet on personal devices. Permission for the connection of personal devices to the school guest wireless network can be granted by the HST in specific circumstances (e.g. for the constant and safe monitoring of the blood sugar levels of a child with diabetes). Any such use will be limited to the purpose for which permission is granted.

Trips / events away from school

For school trips/events away from school, teachers are permitted to use their mobile phone for the purposes of communicating with the school and, if necessary (e.g. in an emergency), with a child's families/carers/emergency contact. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a family or child accessing a teacher's private phone number.

The school office will use a central text message and email distribution service to provide families with any updates about trips as necessary (e.g. an unexpected late return).

Searching and confiscation

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

Full details of the school's search procedures are available in the [school Behaviour Policy].

Appendix A – Roles

Please read the relevant roles & responsibilities section from the following pages.
All school staff must read the "All Staff" section as well as any other relevant to specialist roles
Roles:

- All Staff
- Co-Headteachers
- Designated Safeguarding Lead
- Governing Body, led by Safeguarding Link Governor
- Wellbeing Lead
- Computing Lead
- Subject leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Children
- Families
- External groups including family associations

All staff

- Be aware of safeguarding provisions for **home-learning** and **remote-teaching technologies**.
- Recognise that **RSHE** (Wellbeing) is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1 and Annex A of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for HST and those working directly with children, it is good practice for all staff to read all three sections)
- Read and follow this policy in conjunction with the school's main Safeguarding Policy
- Record online safety incidents by reporting them to the DSL or OSL and, if deemed necessary by the DSL, on CPOMS
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the Staff Acceptable Use Policy and Staff Handbook
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the Wellbeing and computing curricula, 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 children)
- 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)
- Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or children bypassing protections.

Co-Headteachers – Rebecca Shelley & Suzanne Kelly

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 technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Ensure that policies and procedures are followed by all staff
- 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
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- 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 children in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of children, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead – Kayley Dunn

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

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE
- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and

open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to children confused

- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - In 2023/4 this must include filtering and monitoring and help them to understand their roles
    - 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 (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
    - cascade knowledge of risks and opportunities throughout the organisation
    - safecpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- 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 safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the Co-Headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- 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 families, including hard-to-reach families – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding 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 children to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- 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 families.
- Work with the Co-Headteacher to ensure the school website meets statutory DfE requirements

Governing Body, led by Online Safety / Safeguarding Link Governor – Suzannah Flanagan

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
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging families and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and Co-Headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- 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 and now also reminders about filtering and monitoring
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

Wellbeing Lead – El Jeffrey

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 children' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help children to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where children need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" to complement the computing curriculum
- Work closely with the DSL/OSL 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 – April Williams

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/OSL 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 RSHE curriculum, and model positive attitudes and approaches to staff and children alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in their context
- Work closely with the DSL/OSL 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/IT Technician – Geoff Blyth/Jack Clancey

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 when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- 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) to support their role as per the new DfE standards, protections for children in the home and remote-learning.
- 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 the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- Monitor the use of school technology and online platforms and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO) – Judicium

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- 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 2023, "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."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until the child is aged 25 or older)'. However, some local authorities require record retention until 25 for all child 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.
- 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
- 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 child. The same applies to any private/direct communication with a child.

Children

Key responsibilities:

Read, understand, sign and adhere to the child acceptable use policy

- 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 family were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology

- 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 AUPs 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

Families

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the children's AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, children or other families
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns to school staff.
- Support the child during remote 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. The background could be changed/blurred where possible.

External groups (e.g. those hiring the premises) including parent associations – Ridgeway PTCA

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, children or other families