



Riversdale Primary School

A nurturing, ambitious and values led school.

ONLINE SAFETY POLICY

DATE: 1st September 2026

REVIEW DATE: 31st August 2027

INTRODUCTION

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE), '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 will always follow the school's safeguarding and child protection procedures.

KEY PEOPLE/DATES

ROLE	STAFF
Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Tracey Tattersall senco@riversdale.wandsworth.sch.uk
Deputy Designated Safeguarding Leads / DSL Team Members	Steven Sousa head@riversdaleschool.org.uk Helen Barnard hbarnard@riversdaleschool.org.uk Scott Parker sparker@riversdaleschool.org.uk
Link Governor for Safeguarding	Martine Thompson mthompson@riversdaleschool.org.uk
Curriculum leads with relevance to online safeguarding and their role	Steven Sousa head@riversdaleschool.org.uk
Network manager/other technical support	Andrew King it@riversdale.wandsworth.sch.uk

WHO IS IT FOR & WHEN IS IT REVIEWED?

This policy is a living document, subject to full annual review and amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place, why they are, and how the policy affects day-to-day practice.

Acceptable Use Policies for different stakeholders help with this. Any changes to this policy will be immediately disseminated to all the above stakeholders.

WHO LEADS ONLINE SAFETY?

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

WHAT WERE THE MAIN ONLINE SAFETY RISKS IN 2025/2026?

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

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

- **CONTACT:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,
- **CONDUCT:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **COMMERCE:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

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

ONLINE SAFEGUARDING TRENDS AT RIVERSDALE PRIMARY SCHOOL

In our school over the past year, we have identified a number of recurring issues relating to children's use of devices, online platforms and social media outside school. These local trends are consistent with national research published during 2025/26 and inform our curriculum, safeguarding practice and work with parents and carers.

Use of Roblox and other online gaming platforms. We are increasingly aware of pupils accessing online games at home with limited adult supervision. These platforms can involve interaction with other users, user-generated content, in-game purchases and communication functions, creating potential risks relating to inappropriate content, contact with unknown individuals, bullying and commercial pressure.

This is particularly relevant in the primary phase: Ofcom found that 51% of 8–14-year-olds had used Roblox in the previous four weeks, while 72% of 8–17-year-olds played games online. Among children who game online, 55% reported playing at least sometimes with people they had only met online, with one in five doing so all or most of the time. Nationally, parents' principal gaming concerns were children talking to strangers (64%), being bullied by other players (60%), exposure to inappropriate content such as violence, bad language or disturbing material (59%) and pressure to make in-game purchases (51%).

Access to YouTube and other video-sharing platforms. We have encountered incidents where pupils have viewed material at home that is not appropriate for their age, including content containing unsuitable themes or language. This reflects the very high level of use nationally. YouTube, excluding YouTube Kids, was the most commonly reported online service among children in Ofcom's 2025/26 research, used by 66% of 8–14-year-olds in the previous four weeks. Children aged 4–15 spent an average of 7 hours and 7 minutes per week watching YouTube during 2025, an increase of 8% from the previous year. Ofcom also found that 69% of parents were concerned about their child encountering age-inappropriate adult or sexual content online, rising to 77% among parents of 6–7-year-olds.

Under-age use of social media and messaging platforms. We have seen some issues arising from pupils' use of platforms including WhatsApp and Snapchat outside school, sometimes without sufficient adult supervision, as well as inappropriate use of social media or messaging groups involving parents and carers. Such activity can have a direct impact on relationships, behaviour and wellbeing within school even where the original interaction took place at home. Ofcom found that 58% of 8–14-year-olds had used WhatsApp in the previous four weeks. Although most major social-media services set a minimum age of 13, only 32% of parents nationally correctly identified 13 as the usual minimum age, and a quarter of parents said they would allow their child to have a social-media profile before reaching the stated minimum age; this rose to 30% among parents of 10–12-year-olds.

We recognise that online risk is not experienced equally by all children and that some pupils may require more explicit teaching, greater adult support or individualised approaches to recognising and responding to online harm. Ofcom found that children with a limiting or impacting condition were substantially more likely than those without one to report encountering something 'worrying or nasty' online in the previous month (28% compared with 15%). They were also more likely to report nasty or hurtful behaviour directed towards themselves (38% compared with 19%). This reinforces the importance of ensuring that online-safety education is accessible, appropriately adapted and revisited regularly.

These trends reinforce the importance of a whole-school approach to online safety. Riversdale uses safeguarding information, CPOMS records, filtering and monitoring information, pupil voice and concerns raised by families to identify emerging patterns. Where issues arise, these are responded to through safeguarding procedures and, where appropriate, used to inform curriculum teaching, targeted pupil support and communication with parents and carers.

HOW WILL THIS POLICY BE COMMUNICATED?

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

- Posted on the school website,
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year),
- Integral to safeguarding updates and training for all staff,
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school,
- Discussed in parent webinars/workshops.

CONTENTS

INTRODUCTION	2
KEY PEOPLE/DATES	2
WHO LEADS ONLINE SAFETY?	2
WHAT WERE THE MAIN ONLINE SAFETY RISKS IN 2025/2026?	2
HOW WILL THIS POLICY BE COMMUNICATED?	3
CONTENTS	5
OVERVIEW	7
Aims	7
Scope	7
ROLES AND RESPONSIBILITIES	7
EDUCATION AND CURRICULUM	7
HANDLING SAFEGUARDING CONCERNS AND INCIDENTS	8
Nudes & Semi Nudes	9
Priority Areas	10
Child-On-Child Sexual Violence and Sexual Harassment	10
Misuse of School Technology (Devices, Systems, Networks or Platforms)	10
Social Media Incidents	11
CCTV	11
EXTREMISM	11
DATA PROTECTION AND CYBER SECURITY	11
APPROPRIATE FILTERING AND MONITORING	11
MESSAGING/COMMENTING SYSTEMS (INCL. EMAIL, LEARNING PLATFORMS & MORE)	13
Authorised Systems	13
Behaviour/Usage Principles of Messaging/Commenting Systems	13
USE OF GENERATIVE AI	13
ONLINE STORAGE OR LEARNING PLATFORMS	14
SCHOOL WEBSITE	14
DIGITAL IMAGES AND VIDEO	14
SOCIAL MEDIA	15
Our SM Presence	15
Staff, Pupils' and Parents' Social Media Presence	15
DEVICE USAGE	16
Personal Devices Including Wearable Technology and Bring Your Own Device (BYOD)	16

Use of School Devices	17
Trips/Events Away From School	17
Searching and Confiscation	17
APPENDIX A – ROLES	19
All staff	19
Headteacher/Principal – Steven Sousa	19
Designated Safeguarding Lead – Tracey Tattersall	20
Governing Body, led by Online Safety / Safeguarding Link Governor – Martine Thompson	21
RHW (PSHE/RSHE) Lead – Steven Sousa	21
Computing Lead – Scott Parker	21
Subject/Phase Leaders	22
Network Manager/other technical support roles – Andrew King & Cygnet IT Services	22
Data Protection Officer (DPO) – Gary Hipple (Wandsworth)	22
Volunteers and Contractors	23
Pupils	23
Parents/carers	23
External Groups (E.G. Those Hiring the Premises) Including Parent Associations	23
APPENDIX B: THE NATIONAL LANDSCAPE OF ONLINE SAFETY	24

OVERVIEW

Aims

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

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

Scope

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

ROLES AND RESPONSIBILITIES

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

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

EDUCATION AND CURRICULUM

Despite the risks associated with being online, Riversdale Primary School recognises the opportunities and benefits of technology for children. Technology is a fundamental part of adult life and developing the competence to understand and use it safely is important to children's later outcomes. The choice to use technology in school will always be driven by pedagogy, inclusion and safeguarding. Staff will scaffold pupils' use of technology appropriately and make reasonable adaptations so that pupils with SEND can participate safely and successfully.

Riversdale provides a carefully sequenced online-safety curriculum that develops knowledge, skills and behaviours over time, builds on prior learning and is appropriate to pupils' age, development and needs.

At Riversdale Primary School, pupils discuss online safety through Computing, RHW, safeguarding and wider curriculum opportunities. Teaching is revisited throughout the year and is supplemented when emerging issues, incidents or changes in technology make this necessary. This helps ensure that online-safety teaching remains current and responsive to pupils' experiences and needs.

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

Online-safety teaching is assessed in age-appropriate ways so that staff can identify what pupils understand, where misconceptions remain and where additional teaching or intervention is needed. Curriculum review draws on safeguarding information, pupil voice and evidence from teaching and learning.

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

- Relationships, Health and Wellbeing education which encompasses the RSHE/PSHE objectives;
- Computing.

However, it is the role of ALL staff to identify opportunities to thread online safety through school life, both within and beyond the classroom, and to make appropriate use of unexpected learning opportunities as they arise. At Riversdale, online safety is mapped primarily through Computing and RHW, with relevant links made through safeguarding, behaviour, personal development and the wider curriculum.

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

Annual reviews of curriculum plans and schemes of work, including provision for pupils with SEND, are used to strengthen online-safety education. This sits within an annual online-safety audit led by the DSL, Tracey Tattersall, working with the Headteacher, Computing Lead, RHW Lead and technical support.

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

We recognise that nationally, children with SEND may be at increased risk of online harm and may require more explicit, adapted teaching. At Riversdale Primary School, online-safety teaching is adapted for pupils' communication, cognition, sensory, regulation and developmental needs, including pupils in the Resource Base. This may include visual supports, repetition, modelling, supported practice, individual risk assessment and targeted intervention. Where necessary, additional technical controls may also be considered for individual pupils.

We communicate with parents and carers about how we support pupils with online safety through this policy, curriculum information, newsletters and direct school communications. We also share guidance when particular issues or emerging risks require additional parental awareness. Communication will be made accessible where required.

HANDLING SAFEGUARDING CONCERNS AND INCIDENTS

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

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

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

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse and Sexual Harassment procedures within the Safeguarding and Child Protection Policy
- Behaviour & Anti-Bullying Policy
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection and Information Security Policy, privacy notices, consent arrangements and associated documentation
- Cyber security arrangements within the Data Protection and Information Security Policy and technical procedures
- This Online Safety Policy, including the school's approach to generative AI.

This school commits to taking all reasonable precautions to safeguard pupils online, but the internet can never be 100% safe (as stated in KCSIE), and we recognise that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school).

Any suspected online risk or infringement should be reported to the DSL as soon as possible on the same day. The reporting member of staff will ensure that a record is made on CPOMS. This includes concerns arising from filtering and monitoring systems. Where there is an immediate risk of harm, staff must also speak directly to a DSL without delay.

As required by the Children's Wellbeing and Schools Act (2026), teachers must report concerns of child sexual abuse, including abuse facilitated by or taking place online, such as non-contact abuse and image sharing. All staff must report such concerns without delay to the DSL.

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

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

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

Where staff become aware of a safeguarding concern outside normal school hours, they should record it on CPOMS and follow the school's safeguarding procedures. Where a child may be at immediate risk, staff must not wait for the school to reopen before contacting the appropriate emergency or safeguarding service.

Staff receive online-safety updates through safeguarding training, induction and regular staff briefings. Scenario-based training may be used where this supports staff confidence in recognising, responding to and recording online-safety concerns.

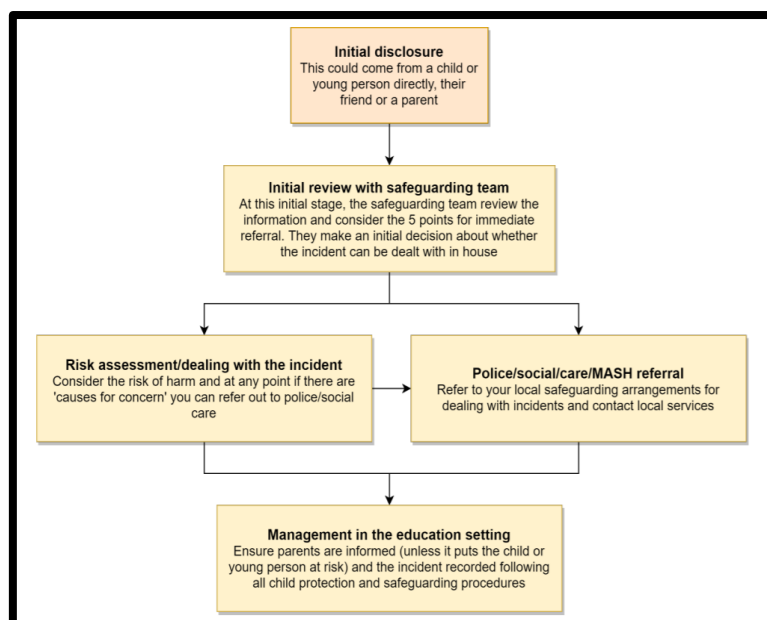
Nudes & Semi Nudes

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

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

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

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



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

SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?

A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

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



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

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



Priority Areas

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

Child-On-Child Sexual Violence and Sexual Harassment

At Riversdale, concerns about child-on-child sexual violence, sexual harassment, harmful sexual behaviour or sexually harmful online activity are treated as safeguarding concerns. They are recorded on CPOMS, considered alongside the school's safeguarding and behaviour procedures and responded to in a way that prioritises the safety and support of all children involved.

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 expectations are defined in the relevant Acceptable Use Policies as well as in this document, including the sections relating to professional and personal use of school platforms, networks, devices and other technology.

Where pupils contravene these rules, the Behaviour Policy will be applied. Where adults contravene these rules, action will be taken in line with the Staff Code of Conduct and, where appropriate, disciplinary or safeguarding procedures.

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

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

Social Media Incidents

Social media incidents involving pupils may be safeguarding concerns and will be treated as such where harm is caused or there is a risk of harm. Staff must follow the Safeguarding and Child Protection Policy, alongside relevant Acceptable Use, Behaviour and Anti-Bullying procedures.

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Riversdale Primary School may request that the content is removed and expect this to be actioned promptly. The police or other agencies may be contacted where an offence may have been committed or there is a safeguarding concern.

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.

CCTV

Riversdale Primary School uses CCTV to support the safety and security of pupils, staff, visitors and the school site.

CCTV is positioned in external areas of the school. It is not used for routine monitoring of teaching or learning and is operated proportionately for safeguarding, security and site-management purposes.

CCTV use is managed in accordance with data-protection legislation, the school's Data Protection and Information Security Policy and relevant privacy information. Cameras are positioned and used in a way that seeks to protect privacy and dignity.

Access to CCTV footage is restricted to authorised staff and footage is stored securely and retained only for as long as required under the school's retention arrangements, unless it is needed for a safeguarding, disciplinary, insurance or legal matter.

Appropriate signage and privacy information are used to make the school community aware that CCTV operates on the site.

EXTREMISM

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

DATA PROTECTION AND CYBER SECURITY

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Data Protection and Information Security Policy and associated cyber-security procedures. There is a close relationship between data protection, cyber security and the school's ability to safeguard children effectively. The school takes account of the DfE Cyber Security Standards for Schools and Colleges.

APPROPRIATE FILTERING AND MONITORING

The DSL has lead responsibility for filtering and monitoring and works closely with Andrew King and Cygnet IT Services to implement and review the DfE Filtering and Monitoring Standards.

We provide appropriate filtering and monitoring, as outlined in KCSIE, across school systems and devices.

Our network filtering system is LGfL SchoolProtect. Filtering settings are reviewed with technical support so that inappropriate and harmful content is restricted while avoiding unnecessary over-blocking of legitimate curriculum content.

Staff are reminded of filtering and monitoring arrangements at induction, through start-of-year safeguarding training, Acceptable Use Policies and subsequent updates. Staff must report concerns about inappropriate access, possible attempts to bypass filtering, under- or over-blocking, or unexpected content to the DSL and/or IT support. Safeguarding concerns must also be recorded on CPOMS.

Technical and safeguarding colleagues work together to carry out an annual review and regular checks of filtering and monitoring. Where patterns or concerns are identified, these are considered alongside safeguarding and curriculum information so that technical controls, teaching and pastoral responses can be adjusted where necessary.

We carry out regular checks of filtering and monitoring arrangements, including half-termly checks where appropriate, and an annual review as part of the school's online-safety audit. Records are maintained by the DSL and relevant technical colleagues and are available for governance oversight.

We use LGfL guidance and templates, alongside school and technical records, to support filtering checks and the annual online-safety review.

Staff may use only generative AI tools that have been approved by the school and must follow the requirements in the 'Use of generative AI' section of this policy. Pupils are not permitted to access or use generative AI tools in school. Where generative AI functionality is embedded within another approved service, access will be risk assessed and restricted or disabled where appropriate.

Safe Search settings are enforced on supported search services on school-managed devices. Filtering settings are reviewed with Cygnet IT Services. Staff remain responsible for supervising pupils' searching because filtering and Safe Search cannot guarantee that all content, including AI-generated summaries, will be accurate or appropriate.

Pupils use school-approved search tools and websites appropriate to the learning activity and their age. Access to other search services may be restricted through SchoolProtect where necessary.

YouTube access is managed through the school's filtering arrangements and is used only where staff have judged content to be appropriate for the intended learning. Staff should preview material before use with pupils wherever practicable.

The DSL reviews filtering reports and relevant notifications regularly and takes action where patterns, attempted access or safeguarding concerns are identified. Urgent concerns are acted upon as soon as practicable and recorded through the school's safeguarding procedures where appropriate.

School-managed devices remain subject to school filtering and security controls wherever those controls are technically available. Personal devices are not used by pupils to access the school network unless specifically authorised.

According to the DfE standards, the school should have a plan for how to "monitor pupils when using school-managed devices connected to the internet.

At Riversdale Primary School, technical monitoring arrangements are overseen by the DSL in partnership with Andrew King and Cygnet IT Services. The school reviews the effectiveness of monitoring as part of its filtering and monitoring checks and annual online-safety review.

Where monitoring relates to staff activity, any concern is managed in line with safeguarding allegations, the Staff Code of Conduct, data-protection requirements and appropriate employment procedures. Concerns about a member of staff are reported to the Headteacher; concerns about the Headteacher are referred to the Chair of Governors and/or LADO.

Relevant monitoring alerts and reports are reviewed by the DSL and/or authorised technical staff. The frequency and urgency of review are proportionate to the nature of the alert, with high-risk safeguarding concerns prioritised for immediate action.

Out of hours, our policies are:

- for filtering, technical controls remain in place on school-managed systems and devices where supported; routine report review is undertaken during working periods, with urgent concerns escalated through safeguarding procedures.
- for monitoring, the school does not rely on continuous staff surveillance outside normal working hours. Where an urgent safeguarding concern is identified, normal safeguarding and emergency-reporting routes apply.

MESSAGING/COMMENTING SYSTEMS (INCL. EMAIL, LEARNING PLATFORMS & MORE)

Authorised Systems

- Pupils use approved learning platforms including Google Workspace for Education, Century Tech, Times Tables Rock Stars (TTRS) and ReadWorks. Pupils do not have access to school email accounts. Where approved platforms include commenting or communication features, these are used only for educational purposes and under staff oversight.
- Staff and governors use school-provided Google Workspace for Education accounts for school email and school business. Personal email accounts or unauthorised messaging platforms must not be used to communicate with pupils or parents/carers, or to share school or pupil data.

School information and communication are managed through approved systems, including Google Workspace for Education, Arbor and CPOMS where appropriate to the purpose. Safeguarding information must be recorded and shared through CPOMS and the school's safeguarding procedures, not through informal messaging channels.

These systems are centrally managed by the school and/or authorised IT partners and can be administered, audited or reviewed where required. This supports safeguarding, privacy, accountability and compliance with UK data-protection law.

Any new platform or app with communication facilities, pupil logins or the capacity to store school or pupil data must be approved in advance by the Headteacher in consultation with the DPO, DSL and/or IT support as appropriate, and must be capable of being managed safely by the school.

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

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the circumstances of the incident will determine whose remit this is) should be informed immediately.

Staff must take particular care where devices contain both personal and school accounts, for example Google accounts, to ensure information is not uploaded, shared or emailed using a personal account in error.

Behaviour/Usage Principles of Messaging/Commenting Systems

More detail is set out in the school's Acceptable Use Policies, Behaviour Policy, Staff Code of Conduct and Data Protection and Information Security Policy.

Appropriate behaviour is expected at all times by all users, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Data-protection principles will be followed at all times in school communications, in line with the Data Protection and Information Security Policy and using only authorised systems.

Pupils do not have school email accounts. Staff school email accounts are provided for professional school use. Limited incidental personal use by staff must remain reasonable, lawful and consistent with the Staff Code of Conduct, Acceptable Use Policy and data-protection expectations. Users should understand that use of school-managed systems may be monitored or audited where lawful and necessary.

USE OF GENERATIVE AI

At Riversdale Primary School, we acknowledge that generative AI platforms are increasingly common in adult life and may also affect pupils through services used outside school. We therefore take a cautious, safeguarding-led approach to their use.

- The use of generative AI in our setting is carefully managed to protect users, personal data, confidentiality, intellectual property and the quality of teaching and learning.
- Staff may use only school-approved generative AI tools. Where an account is required, staff must use an approved school account and must never enter personal, special-category, safeguarding or confidential information about pupils, families or staff into a generative AI system unless the school has explicitly approved that use following appropriate data-protection assessment.

- Staff remain professionally accountable for any material produced with generative AI. Outputs must be checked for accuracy, bias, suitability, copyright and safeguarding concerns and must not replace professional judgement.
- Pupils are not permitted to access or use generative AI tools in school. The curriculum will nevertheless teach pupils, in an age-appropriate way, about AI-generated content, misinformation, deepfakes, privacy, bias and the importance of checking information critically.
- We recognise that pupils may encounter generative AI outside school. Teaching and parent/carers guidance will therefore address both potential benefits and risks, including data privacy, misinformation, cyberbullying, deepfakes, manipulated intimate imagery and unsafe or inappropriate chatbot interactions.
- Using generative AI to misrepresent a pupil's own work, to create harmful or abusive content, or to bypass school expectations is prohibited and will be addressed through the Behaviour Policy and safeguarding procedures as appropriate.
- Riversdale does not permit pupil use of generative AI. Staff use is limited to approved tools and approved purposes. Approval of a new AI-enabled product will consider safeguarding, age restrictions, data protection, security, educational value and the DfE Generative AI Product Safety Standards where applicable.
- Staff may use approved generative AI to support professional tasks such as planning or resource development, but must check outputs carefully and must not upload pupil work, personal data or confidential school information unless that specific use has been formally approved.
- Approval of new AI platforms sits with the Headteacher, informed by the DSL, DPO and IT support as appropriate. A Data Protection Impact Assessment will be completed where required.
- AI meeting assistants, transcription tools and automated notetakers must not be used for school meetings unless specifically approved in advance, with clear consideration of safeguarding, confidentiality, consent and data protection.
- Pupils may learn about generative AI and AI-generated content as part of digital literacy and online safety, but they do not use generative AI tools themselves in school.
- AI education will be age appropriate and linked to Computing, RHW and wider digital literacy. Pupils will be taught to question accuracy, identify manipulation and understand that AI-generated material may be biased, false or unsafe.
- Staff will receive updates and guidance as the school's use of approved AI develops. Parents/carers will be provided with information where new technologies or emerging risks materially affect pupils.

ONLINE STORAGE OR LEARNING PLATFORMS

All the principles outlined above also apply to any online system used for school business, storage, collaboration, learning or teaching. At Riversdale Primary School this includes Google Workspace for Education, Arbor, CPOMS, Century Tech, Times Tables Rock Stars (TTRS) and ReadWorks.

Any new platform will be approved by the Headteacher in consultation with the DPO, DSL and/or IT support as appropriate.

SCHOOL WEBSITE

The school website is a key public-facing information portal for existing and prospective families and has important statutory and reputational functions. The Headteacher has overall responsibility for website compliance and may delegate day-to-day content updates to appropriate staff.

The website is maintained through the school's approved website provider. Technical or content changes are managed only by authorised staff or suppliers.

Where staff submit information for the website, they must respect copyright law. Sources must be credited where required and material must only be used where the school has permission or a lawful basis to do so. If in doubt, staff should check with the Headteacher or DPO before publication.

DIGITAL IMAGES AND VIDEO

When publishing images on the school website or in marketing materials, Riversdale takes a safeguarding-led and data-minimisation approach. We avoid unnecessary high-resolution close-up images of identifiable pupils, favour group or activity-focused images where appropriate, and consider the risk of images being copied or manipulated using AI. Publication is always subject to the school's consent and safeguarding arrangements.

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

Whenever a photo or video is taken, the member of staff responsible must check the school's current consent information before using it for publication or wider sharing. Storage and retention must follow the Data Protection and Information Security Policy.

No member of staff may use a personal phone, tablet, camera or other personal device to photograph or record pupils. Riversdale provides school phones for authorised photography and video. These devices remain on the school site and are cleared at the end of each day once images have been transferred to approved school storage or are no longer required.

School photographs and videos are stored only in approved school systems, including authorised Google Workspace for Education storage where appropriate, and are retained in line with the school's Data Protection and Information Security Policy. Any concern about an image or recording must be reported to the DSL.

Parents/carers must not covertly film or record interactions with pupils or adults in school or near the school gates, and must not share images of other people's children on social media without appropriate permission. At school events, any photography or filming must follow the expectations communicated by the school.

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

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

SOCIAL MEDIA

Our SM Presence

Riversdale 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.

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

Steven Sousa (Headteacher) is responsible for managing our Instagram social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, Pupils' and Parents' Social Media Presence

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

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

If parents/carers have a concern about the school, we ask them to contact us directly and privately so that the matter can be addressed. Where an issue is not resolved, the school's published Complaints Procedure should be followed. Posting complaints on social media may make resolution more difficult and may cause unnecessary distress to pupils, families or staff.

Many social media platforms have a minimum age of 13. As a primary school, Riversdale does not encourage or condone underage use and asks parents/carers to respect platform age requirements and parental-control arrangements. Where an online incident involving a pupil affects their safety, wellbeing or education, the school will respond appropriately regardless of where or on which platform it occurred.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will explore online behaviour,

how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long and when. The school will share age-appropriate online-safety guidance and signpost families to trusted resources when helpful. Riversdale Primary School does not currently operate active official social media accounts. Parents/carers should communicate with the school through the school office, Arbor and other approved school communication channels rather than social media.

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

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

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher 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 must not bring the school or profession into disrepute. They should use appropriate privacy settings, avoid inappropriate sharing or oversharing, and must never discuss confidential school matters or pupils on social media. Staff must not create social-media or influencer content in school, about pupils, or using identifiable school material without explicit permission from the Headteacher.

DEVICE USAGE

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

Personal Devices Including Wearable Technology and Bring Your Own Device (BYOD)

Pupils

- Our approach to pupils using mobile phones is in line with DfE guidance. Pupils should not bring mobile phones to school unless this has been agreed because they travel home independently. In practice, this applies to pupils in Years 5 and 6 who have permission to go home alone. Phones must be handed to staff at the start of the school day and are returned at the end of the day. They must not be used during the school day. Misuse will be managed in line with the Behaviour Policy and safeguarding procedures where relevant.
- Phones collected from pupils are stored securely for the school day and must be switched off or otherwise made incapable of recording or transmitting while in school custody.
- Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- Personal recording devices, such as smart glasses, are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

Staff

- They should keep their mobile phones on silent and only use them in private staff areas during school hours. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- See also the 'Digital images and video' section of this document and the school data protection cyber security policies. Child/staff data should never be downloaded onto a private phone.
- Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

Where a pupil or member of staff requires access to a personal mobile device for a medical or accessibility reason, arrangements will be agreed on an individual basis through an appropriate risk assessment and, where relevant, in consultation with parents/carers and health professionals.

Volunteers, Contractors, and Governors

- They should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member of staff.
- Other personal recording devices, such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

Parents

- Parents/carers are asked to keep phones put away when on the school site and to avoid using them around pupils unless there is a clear and appropriate reason.
- They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events.
- Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- We do not allow Apple AirTags or similar devices in school. Please note that it is against the terms and conditions of these products to use them to track a child.
- It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device. Other personal recording devices such as smart glasses are not permitted in school without written permission.

Use of School Devices

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

Access to the school Wi-Fi/network is restricted to authorised users and devices. Personal devices may connect only where this has been specifically authorised and must comply with the school's Acceptable Use and data-protection requirements. Network use is subject to filtering and appropriate monitoring.

School devices for staff and pupils are restricted to school-approved apps and software and must be used in line with the Acceptable Use Policies, Staff Code of Conduct and Behaviour Policy. Users must not use VPNs or any other method to bypass school filtering or security controls.

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

Trips/Events Away From School

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

If on trips, pupils are encouraged to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school. Therefore, staff are responsible for risk assessing and managing such situations and should seek advice from the DSL where necessary.

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

Where staff communicate with parents/carers during trips or events, they must use authorised school systems or a school duty phone wherever possible. Personal contact details must not be disclosed unless an emergency makes this unavoidable.

Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by the Headteacher have a statutory power to search pupils and property on school premises in the circumstances set out in law and

guidance. This can include mobile phones and other devices where there is a lawful basis and reasonable suspicion that prohibited, illegal or harmful material may be present.

Full details of the school's searching, screening and confiscation procedures are set out in the 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**
- **Headteacher/Principal**
- **Designated Safeguarding Lead**
- **Governing Body, led by Online Safety / Safeguarding Link Governor**
- **PSHE / RSHE Lead/s**
- **Computing Lead**
- **Subject / aspect leaders**
- **Network Manager/technician**
- **Data Protection Officer (DPO)**
- **Volunteers and contractors (including tutor)**
- **Pupils**
- **Parents/carers**
- **External groups, including parent associations**

All staff

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

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

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

Headteacher/Principal – Steven Sousa

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 the school implements and makes effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL— in particular, understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the Designated Safeguarding Lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Take overall responsibility for data management and information security, ensuring the school’s provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.

- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead – Tracey Tattersall

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

- The DSL should “take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure “An effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE’s standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out an annual review and regular checks on filtering and monitoring to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication, and that the DSL’s clear overarching responsibility for online safety is not compromised or messaging to pupils is confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is updated annually.
 - This must include filtering and monitoring, and help them to understand their roles.
 - All staff must read and understand KCSIE Part 1 - translations are available in 13 community languages at [kcsietranslate.lgfl.net](https://www.kcsietranslate.lgfl.net)
 - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates about online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework ‘[Education for a Connected World – 2020 edition](#)’) and beyond, in wider school life.
- Promote awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.
- Communicate regularly with SLT and the safeguarding governor/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, e.g. a survey to facilitate disclosures and an online form on the school home page about ‘something that’s 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 parents.

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

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

RHW (PSHE/RSHE) Lead – Steven Sousa

Key responsibilities:

As listed in the ‘all staff’ section, plus:

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

Computing Lead – Scott Parker

Key responsibilities:

As listed in the ‘all staff’ section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within Computing.

- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject/Phase 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 pupils alike.
- Consider how the UKCIS framework 'Education for a Connected World' and 'Teaching Online Safety in Schools' can be applied in your context.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject-specific action plans also have an online safety element.

Network Manager/other technical support roles – Andrew King & Cygnet IT Services

Key responsibilities:

As listed in the 'all staff' section, plus:

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and any changes to these systems (especially access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc).
- Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and ensure that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Gary Hipple (Wandsworth)

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not to prevent or limit the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "Data protection laws do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare."
- Note that retention schedules 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 the age of 25 for all pupil records. You should check the requirements in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and Contractors

Key responsibilities:

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

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil Acceptable Use Policy.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental Acceptable Use Policy (AUP), read the pupil AUP and encourage their children to follow it.

External Groups (E.G. Those Hiring the Premises) Including Parent Associations

Key responsibilities:

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

APPENDIX B: THE NATIONAL LANDSCAPE OF ONLINE SAFETY

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

National Online Safeguarding Trends

1. LGFL SENSO MONITORING

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

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

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

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

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

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

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

2. OFCOM'S LATEST RESEARCH

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

Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%. Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".

Social pressures remain high, with 70% of students feeling pressure to be popular on social apps. Negative experiences are common; 23% of 8-17-year-olds personally experienced "nasty or hurtful" behaviour in the last year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).

Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising. This suggests a need for updated curricula that reflect the evolving risks of AI and commercial influence.

3. IWF, CSAM CONCERNS

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

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

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

4. “COM NETWORKS”

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

5. CYBER ATTACKS

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