ONLINE SAFETY POLICY

2026-2027

OUR TRUST PRAYER

Heavenly Father,

Let peace, friendship and love

grow in our schools.

Send the Holy Spirit to give

excellence to our learning,

love to our actions and

joy to our worship.

Guide us to help others,

so that we may all

Learn, Love and Achieve,

Together with Jesus.

Amen

Contents

1. Introduction **Error! Bookmark not defined.**

2. Overview **Error! Bookmark not defined.**

3. Roles and responsibilities **Error! Bookmark not defined.**

4. Education and curriculum **Error! Bookmark not defined.**

5. Handling safeguarding concerns and incidents **Error! Bookmark not defined.**

6. CCTV **Error! Bookmark not defined.**

7. Extremism **Error! Bookmark not defined.**

8. Data protection and cyber security **Error! Bookmark not defined.**

9. Appropriate filtering and monitoring **Error! Bookmark not defined.**

10. Messaging/commenting systems (incl. e-mail, learning platforms & more)**Error! Bookmark not defined.**

11. Use of generative AI **Error! Bookmark not defined.**

12. Online storage or learning platforms **Error! Bookmark not defined.**

13. School website **Error! Bookmark not defined.**

14. Digital images and video **Error! Bookmark not defined.**

15. Social media **Error! Bookmark not defined.**

16. Device usage **Error! Bookmark not defined.**

17. National College Courses 24

Appendix 1 – Roles **Error! Bookmark not defined.**

Appendix B: The National Landscape of Online Safety 33

Review Schedule 36

1. Introduction

1.1 Key people / dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Jennifer Kilshaw
Deputy Designated Safeguarding Leads / DSL Team Members	Alison Barron, Sarah Mitchell, Natalie Rose
Link governor for safeguarding	Claire Halliwell

Curriculum leads with relevance to online safeguarding and their role [e.g. PSHE/RSHE/RSE/Computing leads]	PSHE/RSE – Gillian Higgins Computing – Becky Ward
Network manager / other technical support	Techminder
Date this policy was implemented by school and by whom	Sep 2026

1.2 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.

1.3 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. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy will be immediately disseminated to all the above stakeholders.

1.4 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.

1.5 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.

Current Online Safeguarding Trends

In our school over the past year, 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 pupils: inappropriate use of social media apps, inappropriate access to youtube, Children having access to Whatsapp groups and parents needing support with this, children communicating with one another through games such as Xbox/Playstation, children not always being kind to one another, 'group chats' where some pupils are not included or kicked out and supervision of personal devices when at home, parents are not always talking to children about what they are on.

1.6 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

- 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

2. Overview

2.1 Aims

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

- Setting out expectations for all 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)

2.2 Scope

This policy applies to all members of our 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.

3. Roles and responsibilities

Our 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 Annex 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 annex. All staff have a key role to play in feeding back on potential issues.

4. Education and curriculum

Despite the risks associated with being online, our 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)
- 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.

At our school, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

5. 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
- Anti-Bullying Policy

- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security
- ICT Regulations
- Social Media Policy
- Mobile Phone Policy
- Artificial Intelligence 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 designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS this includes any concerns raised by the filtering and monitoring systems (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 (who will inform LDST's CEO) and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 0800 028 0285.

Our school will actively seek support from other agencies as needed (i.e. Trust DSL, the local authority, School Improvement Liverpool, 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.

Our school will ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

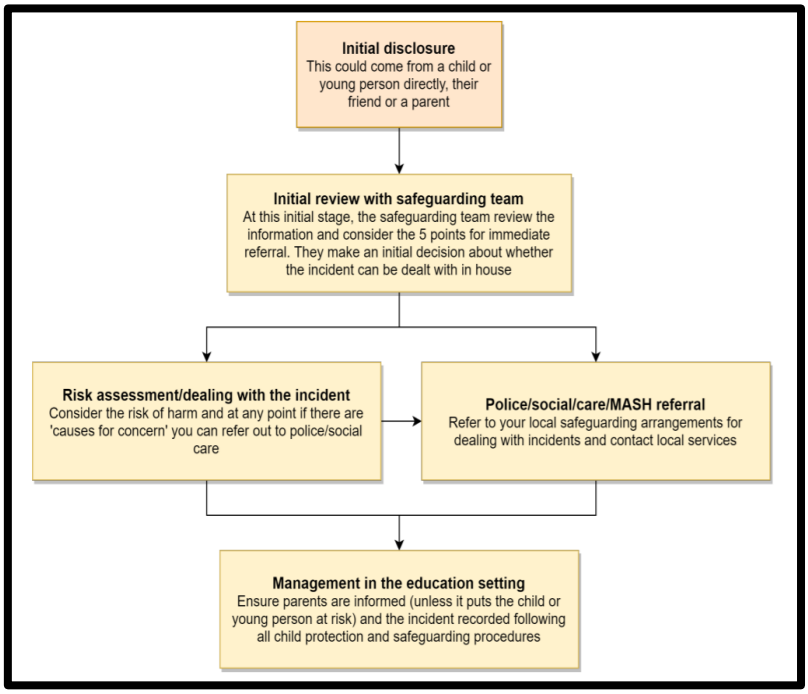
5.1 Nudes – sharing nudes and semi-nudes

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.

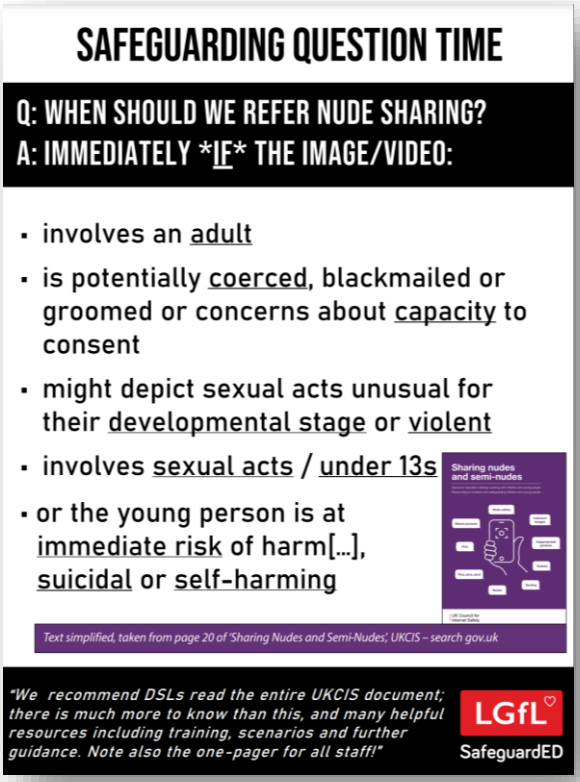
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of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

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

Our 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:



5.2 Priority Areas

5.2.1 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.

5.2.2. Bullying

Online bullying (which may also be referred to as cyber bullying), 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.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

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

5.2.3 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.

5.3 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 safeguarding code for adults/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, our 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.

5.4 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/social media policy/online safety.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or staff safeguarding code for adults/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the school community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), our school will request that the post be deleted and will expect this to be actioned promptly.

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

6. CCTV

Our school uses CCTV for the following purposes:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of pupils, staff, visitors and other members of the public and to act as a deterrent against crime;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in the day-to-day management of the school including ensuring the health and safety of pupils, staff and others;
- for pupil behaviour management (discipline and exclusions); and
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings and associated processes and appeals

We have a CCTV policy which outlines the rationale for use of CCTV, how we balance the use with the right of privacy and how footage is stored, who has access and how long it is stored.

7. Extremism

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

8. Data protection and cyber security

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

9. Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with our Trust Chief Operating Officer and Techminder, our IT support provider, 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 pupils to bypass systems and any potential overblocking. They can submit concerns at any point via e-mail and will be asked for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request dependent on staff roles.

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. For children and young people, we block the generative AI category and only allow specific sites. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines. Find out more at genaisafe.lgfl.net

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

We recommend the use of searching through the SENSO App and block all others.

Our YouTube mode is set to strict.

Out of hours, we use Senso.cloud and the violations are sent in real time. All devices offsite will be monitored but not filtered. When pupil devices are offsite we enable senso.cloud's web filtering policy.

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 checks filtering reports and notifications and 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"

Staff Responsibilities include:

- Monitoring what is on a pupil's screen
- Ensuring that unsuitable material is not accessed
- Teaching topics that could create unusual activity on the filtering logs – and advising the IT support accordingly
- Recognising failure in the software or abuse of the system
- Understanding and resolving unreasonable restrictions that affect teaching and learning or administrative tasks
- Noticing abbreviations or misspellings that allow access to restricted material
- Being aware of concerns raised by pupils

How we protect staff and pupils – filtering and monitoring

Appropriate Filtering System

We protect staff and students by using a mixture of systems. To meet the appropriate filtering requirements, LDST state that a Sophos XGS firewall must be used. This is setup in a way that meets the DfE and LDST IT regulations that apply to all schools, staff and students.

Our Firewalls meets Department for Education (DfE) filtering standards. Techminder configure the firewall to block specific content categories, ensure compliance with IWF and CTIRU lists, and regularly update blocklists. We also, in line with LDST Policies, implement appropriate monitoring and reporting mechanisms.

Block Content Categories: Sophos provides categories that should be blocked, including:

- "Anonymizers" (to prevent bypassing filters).
- "Hacking, Phishing and Fraud".
- "Spam URLs" and "Spyware and Malware".
- "Sexually Explicit", "Nudity", and "Extreme".
- "Peer to peer and torrents" and "intellectual piracy".

•**Enforce Safe Search:** Implement "Safe-Search" on major search engines.

•**Consider Creative Commons:** Utilize a "Creative Commons" license to restrict image results to licensed content, according to a response from Sophos.

•**Malware and Hacking:** Block sites hosting malicious content and bypass tools.

•**Pornography and Explicit Content:** Block categories related to sexually explicit content and nudity.

•**Piracy and Copyright Theft:** Block categories related to illegal distribution of copyrighted material.

Appropriate Monitoring System

To meet the appropriate monitoring requirements set out by the DfE, LDST purchase into a service provided by Senso.Cloud. This is installed on all devices in the Trust. Senso uses AI and keyword algorithms to analyse user actions and content, to detect potential safety risks

Here's how Senso.cloud addresses the DfE's filtering and monitoring standards:

•**Web Content Filtering:**

•Senso.cloud offers a cloud-based, category-based web content filter that blocks access to harmful and inappropriate content. This filtering system is designed to protect students both on and off the school network, even when using devices at home.

•**Monitoring:**

•Senso.cloud also provides monitoring capabilities to help schools track and identify concerning online activity, allowing for timely intervention and support.

•**KCSIE Compliance:**

•Senso's solutions are designed to meet the requirements of KCSIE 2023, which emphasizes the importance of online safeguarding and appropriate filtering and monitoring in schools.

•**DfE Standards:**

•Senso's solutions align with the DfE's standards for filtering and monitoring, which are crucial for maintaining a safe online environment for students.

•**Contextual Alerts:**

•Senso.cloud can provide contextual alerts, allowing schools to react proactively to potentially concerning pupil behavior, communications, or access.

10. Messaging/commenting systems (incl. e-mail, learning platforms & more)

10.1 Authorised systems

- Staff at this school use the e-mail system provided by our Trust for all school e-mails. They **never use a personal/private email account** (**or other**

messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this e-mail system to communicate with parents, external organisations but not with under 18s.

- Staff at this school use school email or Teachers2Parents, Class Dojo

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

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. Approval is to be sought from the Trust Chief Operating Officer.

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 e-mail 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/Data Protection Lead/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

10.2 Behaviour / usage principles of messaging/commenting systems

More detail for all the points below are given in the 15. Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff safeguarding code for adults.

- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

Pupils and staff are allowed to use the e-mail system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their e-mails may be read and the same rules of appropriate behaviour apply at all times. E-mails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination and will be dealt with according to the appropriate policy and procedure.

11. Use of generative AI

At our school, whilst we acknowledge that generative AI tools such as ChatGPT, Canva, Co-Pilot or Gemini for the creation of new text/imagery/code/music etc, are becoming commonly used by both children and adults, our Trust has strict protocols regarding data protection:

- Google Gemini: This is the Trust's only approved secure AI platform. It is the sole platform authorised for creating school promotional materials (such as posters or flyers) that include pupil photos, provided valid image consent is in place.
- Microsoft Copilot: Authorised for general use, provided no personal data (images, names, or identifying information) is uploaded or shared.
- ChatGPT: Not authorised for use under any circumstances.
- General R**ule:** No other AI platform is approved for tasks involving personal data.

- We are aware of and follow the DfE's guidance on this and we follow the subsequent principles:

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

Our school follows the Trust AI Policy which provides further information.

12. 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 cyber security before adopting such a platform or service and at all times when using it. Any new platforms will be approved by the Trust Chief Operating Officer.

13. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations. Our Trust provides a website audit document which our school uses to ensure compliance.

The website is managed by school and hosted by an external provider.

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

14. Digital images and video

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

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

Any pupils shown in public facing materials are rarely identified with more than first name. Occasionally, a pupil/student may be holding a certificate of achievement or work they have produced with their name included – it is this possibility that is detailed in our consent forms. Photo file names/tags do not include full names to avoid accidentally sharing them.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At our school members of staff may occasionally (i.e. only when school devices are temporarily not available or there are insufficient devices) use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network/cloud platform in line with the retention schedule and the school Data Protection Polic. Any concerns about the nature of these images will be reported to the DSL or Headteacher.

Staff and parents are reminded annually about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this can be found in the Data Protection Policy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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

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

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

15. Social media

15.1 Our SM presence

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

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

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

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

15.2 Staff, pupils' and parents' SM presence

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

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 parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

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

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but schools across our Trust regularly deal with issues arising on social media involving pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

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

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Although our school has official social media accounts and will respond to general enquiries about the school, we ask parents/carers not to use these channels, especially not to communicate about their children or to make requests for information (subject access and Freedom of Information Requests).

E-mail is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Where social media is more widely used as part of school life, e.g. when a Facebook class group is allowed, then at least a second unrelated teacher will be part of the group to monitor activity between the teacher and students

As outlined in the Acceptable Use Policies, pupils/students are not allowed[1] to be 'friends' with or make a friend request[2] to any staff, governors, volunteers and contractors or otherwise communicate via social media.

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable 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 14. Digital images and video and consent is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

[1] 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/student or staff member to the school).

[2] 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).

16. 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 which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

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

- The DfE has provided statutory guidance to schools and trusts regarding prohibiting the use of mobile phones and smart technology in schools. Please refer to the LDST Mobile Phone and Smart Device Policy for further information regarding this and any exemptions and reasonable adjustments that may apply. The policy applies to pupils, staff, parents, agency workers, governors and trustees, volunteers, visitors and contractors.
- Where BYOD is allowed, neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

16.2 Use of school devices

Staff and pupils 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 safeguarding code for adults.

Wi-Fi is accessible for use of BYOD, guest networks and school-related internet use/ limited personal use within the framework of the acceptable use policy. All such use is monitored.

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

All and any usage of devices and/or systems and platforms may be tracked.

16.3 Trips / events away from school

For school trips/events away from school, teaching staff will be issued with a school duty phone and this number will be used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teaching staff using their personal phone in an emergency will ensure

that the number is hidden to avoid a parent or pupil accessing a member of staff'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 and therefore staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

Our school will ensure that the authorised systems we use to communicate with parents as outlined within policy include any systems used in exceptional circumstances such as on trips if we notify parents of trip updates or status of arriving back at school and that these are DP compliant.

16.4 Searching and confiscation

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

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

17. National College Courses

Listed below are the Online Safety courses available to staff:

Certificate in Online Safety for Support Staff
Certificate in Online Safety for Teaching Staff
Certificate in Online Safety for SENCOs
Certificate in Online Safety for ICT Leads
Certificate in Online Safety for Governors and Trustees
Advanced Certificate in Online Safety for DSLs & Deputy DSLs
Certificate in Online Safety for Staff | Early Years
Advanced Certificate in Online Safety for Managers & Leaders | Early Years

Appendix 1 – 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.

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main child protection policy, the safeguarding code for adults, staff handbook 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 in 2025) 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 the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher (and CEO in relation to Trustees)

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).
- 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. *LDST has procured online safety training via National Online Safety.*

- 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. LGfL's Safeguarding Shorts: Filtering for DSLs and SLT provides an overview.
- 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 Trust Chief Operating Officer, Trust 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 pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead

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

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on filtering and monitoring. (LGfL's Safeguarding Shorts: Filtering for DSLs and SLT provides a quick overview and there is lots of information for DSLs at safefiltering.lgfl.net and appropriate.lgfl.net).
- As part of this, DSLs will work with technical teams to carry out reviews and 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 confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
    - 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 (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 Trust
- 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 (LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net).
- 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 (see spotlight.lgfl.net for a CPD resource to use with staff and for further support.
- 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 (see LGfL's template with questions to use at onlinesafetyaudit.lgfl.net).
- 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 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 about online safety issues and legislation, be aware of local and school trends (see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter).
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.

- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents (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 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 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.

Governing Body, led by Online Safety /Safeguarding Link Governor

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board.
- Undergo (and signpost all other governors 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 (LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net).
- 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 (there is guidance for governors at safefiltering.lgfl.net).
- 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.

- Work with the DPO, DSL and 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."

PSHE / RSHE Lead/s

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 latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives." [training is available at safetraining.lgfl.net
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" – 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

Key responsibilities:

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

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

Subject Leaders

Key responsibilities:

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

- Look for opportunities to embed online safety in your subject or aspect, especially as part of the 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

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 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 / 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.
- 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 cybersecurity policy are up to date, easy to follow and practicable.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements (the technical team is likely to play at least some role in working with the web team).

Trust Data Protection Officer and Designated Data Protection Lead

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, "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). Please refer to our retention schedules for further information regarding this.
- 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 pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

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

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 PTAs

Key responsibilities:

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

Appendix 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.

Review Schedule

Policy Author	Trust Data Protection Officer
Policy Approver	Trust Chief Operating Officer
Current Policy Version	6.1
Policy Effective From	1st September 2026
Policy Review Date	31st August 2027

Revision Schedule

Version	Revisions	By whom
1.0	Original document produced	DPO
2.0	New version due to significant changes throughout the policy to bring it in line with KCSIE 2020 and COVID-19 remote learning/working requirements. DFO and IT Consultant reviewed and provided technical input.	DPO
2.1	Reviewed in line with KCSIE 2021 – updated throughout. Sexting section and references to sexting updated "sharing nudes and semi nudes", reviewed with consideration to the government's peer on peer sexual abuse investigation, IT support provider section added, all links to other documentation/guidance updated, appendices page changed to "Other documentation/guidance relevant to this policy", pupils changed to pupils/students throughout.	DPO
3.0	Reviewed in line with KCSIE 2022. Policy updated in many areas and sections moved around to make it easier to read. New version.	DPO
4.0	Major updates throughout the policy to reflect KCSIE 2023.	DPO
5.0	Reviewed in line with KCSIE 2024. Policy updated in many areas. There is some added content about use of CCTV (if this is in place), filming in and outside school, use of generative AI and filtering and monitoring.	DPO
6.0	Reviewed in line with KCSIE 2025. Policy updated throughout and simplified with many sections now standardised.	DPO
6.1	Reviewed in line with KCSIE 2026 and updated DfE guidance relating to mobile phones and smart devices.	DPO