# Online Safety Policy

# Al-Noor Voluntary Aided Primary School

| | | |
|---|---|---|
| **Approved by:** | Headteacher | **Date:** Oct 2026 |
| **Signed on behalf of GB** | **N/A** | |
| **Last reviewed on:** | October 2026 | |
| **Next review due by:** | October 2027 | |

# Al-Noor VA Primary School Online Safety Policy - 2026/27

## Introduction

### Key people / dates

| | | |
|---|---|---|
| Al-Noor VA Primary School | Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring | Sayed Miah |
| | Deputy Designated Safeguarding Leads / DSL Team Members | Someera Butt<br>Nusrat Abdulla<br>Ujalah Sultan |
| | Link governor for safeguarding | Akhter Raouf |
| | Link governor for web filtering | Akhter Raouf (Acting Governor) |
| | Curriculum leads with relevance to online safeguarding and their role [PSHE/RSHE/Computing leads] | Nusrat Abdulla - Curriculum Lead<br>Ujalah Sultan - PSHE/RSHE<br>Zaheera Navlakhi Ahmed - Computing Lead |
| | Network manager / other technical support | Zaheera Navlakhi Ahmed |
| | Date this policy was reviewed and by whom | Oct 2026 |
| | Date of next review and by whom | Sep 2027, Zaheera Navlakhi Ahmed |

# Al-Noor VA Primary School Online Safety Policy - 2026/27

## 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' (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

## Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review 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 (see safepolicies.lgfl.net) for different stakeholders help with this. Any changes to this policy will be immediately disseminated to all the above stakeholders.

## Who 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 Al-Noor VA Primary School**

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 students:

- Increase in use of online platforms and chat,
- Pupils using devices without adequate supervision,
- Parents unsure of nature of apps and parental controls/supervision needed.

## How will this policy be communicated?

This policy can only impact upon practice if it is a 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
- Discussed in parent webinars/workshops

## Contents


Introduction 2

- Key people / dates 2
- What is this policy? 3
- Who is it for; when is it reviewed? 3
- Who leads online safety? 3
- What were the main online safety risks in 2025/2026? 3
- How will this policy be communicated? 4

Contents 5

Overview 7

- Aims 7
- Scope 7

Roles and responsibilities 7

Education and curriculum 8

Handling safeguarding concerns and incidents 9

- Nudes & Semi Nudes 10
- Priority Areas 12
- Upskirting 12
- Bullying 12
- Child-on-child sexual violence and sexual harassment 12
- Misuse of school technology (devices, systems, networks or platforms) 12
- Social media incidents 13

CCTV 13

Extremism 13

Data protection and cyber security 14

Appropriate filtering and monitoring 14

Messaging/commenting systems (incl. email, learning platforms & more) 15

- Authorised systems 15
- Behaviour/usage principles of messaging/commenting systems 16

Use of generative AI 16

Online storage or learning platforms 17

School website 17
Digital images and video 18
Social media 19
Our SM presence 19
Staff, pupils' and parents' social media presence 19
Device usage 21
Personal devices including wearable technology and bring your own device (BYOD) 21
Use of school devices 22
Trips / events away from school 23
Searching and confiscation 23
Appendix A – Roles 24
All staff 24
Headteacher/Principal – Ms S. Butt 25
Designated Safeguarding Lead – Mr S. Miah 25
Governing Body, led by Online Safety / Safeguarding Link Governor – Mr A. Raouf 27
PSHE / RSHE Lead/s – Ms. U. Sultan 28
Computing Lead – Ms. Z. Navlakhi Ahmed 28
Subject / aspect leaders 29
Network Manager/ Digital Strategy and Infrastructure Leader other technical support roles – Ms. Z. Navlakhi Ahmed 29
Data Protection Officer (DPO) – LBR Representative 30
Volunteers and contractors (including tutors) 30
Pupils 31
Parents/carers 31
External groups (e.g. those hiring the premises) including parent associations 31
Appendix B: The National Landscape of Online Safety 32

# Overview

## Aims

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

- Setting out expectations for all Al-Noor VA 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 Al-Noor VA 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, Al-Noor VA Primary School recognises the opportunities and benefits for children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, is critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

At Al-Noor VA Primary School we engage our pupils in discussions about online safety and technology use through curricular work not restricted to Computing Lessons but also through assemblies and events. This helps us to ensure that our teaching of online safety is up to date and responsive to children's experiences and needs.

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

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

- Relationships, Sex and Health Education (RSHE) and health (also known as RSE or PSHE)
- Computing

However, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and making the most of unexpected learning opportunities as they arise. The PSCHE and Computing Lead work closely to map links across the pupils learning.

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 / 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 led by DSL alongside the Digital Lead at the school.

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

We recognise that nationally, children with SEND are less likely to receive effective online safety teaching, but are more at risk of being a victim of harm caused online. Therefore, at Al-Noor Primary School, we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children need to protect them from harm and prevent future online harm.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by sharing this policy, sharing the curriculum, including information in newsletters and workshops for parents.

## 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
- Behaviour Development Policy inc Anti-Bullying Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security Policy
- Artificial Intelligence Policy

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

Any suspected online risk or infringement should be reported to the DSL as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern CPOMS for all staff and Record of Concern form for visitors this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

As per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

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

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

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

Outside of term-time the DSL/ Safeguarding inbox in monitored by a delegated member of the safeguarding team. An out of office reply is also set on the generic school email which has full details of how to contact the DSL for urgent matters.

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

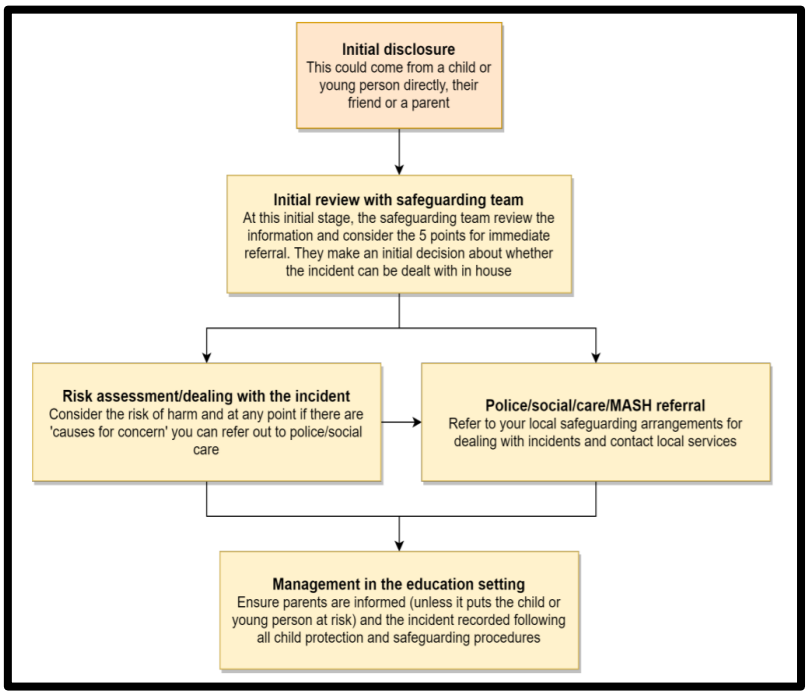
## Nudes & Semi Nudes

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.

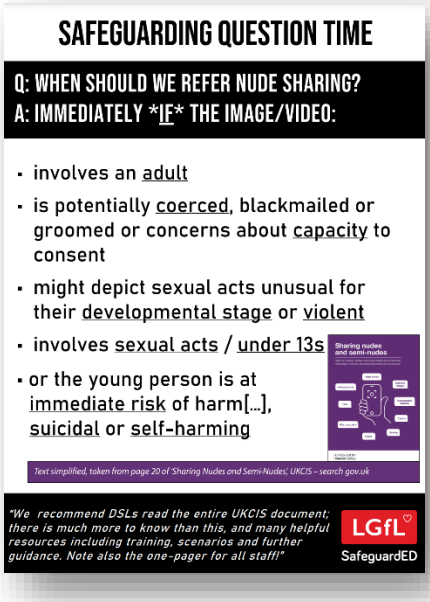
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the Designated Safeguarding Lead (DSL) to first become aware of an incident, and it is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



## Priority Areas

## Upskirting

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 due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing.

## Bullying

Please refer to the school behaviour development policy which covers bullying. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

## Child-on-child sexual violence and sexual harassment

This is a key area as outlined in KCSIE and the Ofsted School Inspection Toolkit (2026).

## 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.

Where pupils contravene these rules, the school behaviour policy will be applied; where adults contravene these rules, action will be taken as outlined in the staff code of conduct/handbook/disciplinary policy.

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 (pupils are not permitted to bring devices to school).

## Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such where there are concerns of harm being caused, and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/Child protection and safeguarding policy and behaviour development policy.

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), Al-Noor VA Primary School will request that the post be deleted and will expect this to be actioned promptly. The police may need to be contacted if an offence is committed.

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

## CCTV

CCTV and other digital image recording will only be used for the purposes identified in the Impact Assessments. This will be communicated via appropriate signage and Privacy Notice. We will ensure that images accessed by, or copies thereof, will be covered by our set purposes and within the law. We are aware that our CCTV processing includes potentially Official-Sensitive information and will take appropriate steps to manage this information as described in this procedure and associated documents.

CCTV recordings are kept for a stated time, in the case of Al-Noor Primary School is 30 days. This is to be stated on the relevant Privacy Notice. After this period has elapsed the recordings will either be recorded over or securely deleted according to the schools documented process. Recordings will only be accessed with a genuine purpose that has been approved by the SIRO and is recorded on the access log. This will include the use of images to review internal matters, images viewed by a third party, passed on to a third party or law enforcement agency or for general maintenance. Signage will be clear, visible from each access point to the site and will state:

- Who is in control of the CCTV system
- A contact telephone number
- A clear representation of the equipment in use.

## Extremism

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

## Data protection and cyber security

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

## Appropriate filtering and monitoring

The DSL has lead responsibility for filtering and monitoring, and works closely with Digital Strategy and Infrastructure Leader at the school as well as our IT service provider Virtual It to implement the DfE Filtering and Monitoring Standards.

We provide 'appropriate filtering and monitoring' (as outlined in KCSIE) in our school.

Our filtering system is called School Protect. For school devices that go off-site, we use HomeProtect filtering. These systems are accredited by the UK Safer Internet Centre.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. We ensure all staff are aware of their responsibility in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. Staff can submit concerns at any point via email to the DSL and Digital Lead 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 an annual review and regular checks of filtering and monitoring, and to ensure that the school responds to issues, considers how to prevent further concerns and integrates with the curriculum.

We carry out termly checks to ensure filtering is operational, functioning as expected, etc., and an annual review as part of an online safety audit of strategy, approach etc. We use templates from LGfL for this documentation.

Where staff use Gen AI, they must be pre-approved by the school as in our AI policy. For children and young people, we block the generative AI category via our filtering and only allow specific pre-approved sites for curricular topics. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate/harmful content can be generated, so we carefully monitor output and limit their use (also in line with DfE guidelines).

Safe Search is enforced on any accessible search engines on all school-managed devices. Please note however that even with Safe Search enforced, AI is embedded in many search engine responses and this presents risk to users in terms of misinformation, bias, hallucinations and inappropriate content.

We recommend the use of google.com.

Our YouTube mode is 'strict' for all guests or staff not logged into their school email domain and for pupils, staff logged in via school domain are on 'moderate' mode. This helps us to limit inappropriate content that is served to pupils.

The Digital Strategy and Infrastructure Leader and DSL checks filtering reports and notifications monthly and takes any necessary action as a result.

Where BYOD is approved for pupils by the Headteacher or Digital Strategy and Infrastructure Leader, 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.

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 Al-Noor VA Primary School, we use LGfL Senso for monitoring.

Monitoring alerts are checked daily throughout the day.

Out of hours, our policies are:

- for filtering devices, we do not monitor them outside of term time or on weekend however upon return from weekend or holidays reports are reviewed.
- for monitoring devices, we do not monitor them outside of term time or on weekend however upon return from weekend or holidays reports are reviewed.

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

### Authorised systems

- Pupils at this school communicate with each other and with staff using Google Classroom only.
- Staff at this school use the email system provided by Google for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use the school email system to communicate with parents as well as via the school MIS approved apps such as Groupcall.

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. This will be approved by the headteacher and reviewed by the IT Manager.

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

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

### Behaviour/usage principles of messaging/commenting systems

- More detail for all the points below are given in the Social media section of this policy as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy https://www.al-noorprimary.org.uk/policies-and-documents and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use, but should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

## Use of generative AI

At Al-Noor VA Primary School, we acknowledge that generative AI platforms (e.g. 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. 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 schools AI policy 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.
- 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.
- The use of any Gen AI in exams, or to plagiarise and cheat, is prohibited, and the Behaviour Development Policy will be used for any pupil found doing so.
- In school, we allow AI Google Gemini use for staff only and for some pupils at a curricular level.
- Staff are permitted in line with our AI policy to use Google Gemini for support in planning of lessons.
- Any new AI platforms of interest to staff for educational use must be requested
- Careful curricular planned use of AI is permitted to teach pupils how to use AI safely in supervised activities.
- Learning about AI is integrated into our curriculum so pupils are aware of benefits of its use, safe use and potential risks.
- Run annual training for staff on use of AI and refreshers.

## 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. In Al-Noor VA Primary School this includes Google Drive.

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 headteacher in liaison with the Digital Strategy and Infrastructure Leader.

## 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 to Z. Navlakhi Ahmed and J. Rahman along with school staff for blog updates.

The website is managed by the school IT team and hosted by Juniper education.

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

## Digital images and video

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

- Photographs/Videos for assessment purposes
- Photographs/Videos for use in school publications
- Photographs/Videos for use on school website
- Photographs/Videos for use on social media – Facebook and X (formerly Twitter)
- Photographs/Videos for use within school premises
- Photographs/Videos to support learning activities
- Photographs and videos by local and national media

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

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

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 Al-Noor VA Primary School; members of staff are provided with school iPads to take photos of pupils in the event this is not available they will seek headteacher authorisation to 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 google drive in line with the retention schedule of the school Data Protection Policy. S. Butt is responsible for checking images/video on all school devices annually. Any concerns about the nature of these images will be reported to the DSL.

Parents must **not** covertly film or record any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media, as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information).

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

Al-Noor VA Primary School works on the principle that if we don't manage our social media reputation, someone else will.

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

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

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

Z. Navlakhi Ahmed and J. Rahman are responsible for managing X-Twitter/Facebook/and other 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 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 https://www.al-noorprimary.org.uk/policies-and-documents 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 but the school sometimes deals 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, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will explore online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentonlinesafety.lgfl.net and parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the school has an official Facebook and X-Twitter account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children. Email 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

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

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

** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the school).*

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

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

See the previous section on image sharing.

## 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**

- 'We are a mobile-free school and no phones are allowed at any time by pupils. 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. Our approach to pupils using mobile phones is in line with DfE, Mobile Phone Guidance
- Other personal recording devices such as smart glasses are not permitted in school. It is forbidden to take secret photos, videos or recordings of teachers or students, including remotely, with any device.

**All staff who work directly with children**

- 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.

**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**

- Are asked to leave their phones in their pockets and turned off when they are on site.
- They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. 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 or on school trips and excursions. 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.

Guest Wi-Fi is accessible to staff and guests for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored. Where BYOD is allowed, this is for staff only when approved by the Headteacher or Digital Strategy and Infrastructure Leader, 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.

Where school devices are permitted to be taken offsite by staff or students they are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning only.

All and any usage of devices and/or 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.

## 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 https://www.al-noorprimary.org.uk/policies-and-documents

## 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/ Digital Strategy and Infrastructure Leader
- 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 (available in the important document folder shared with all staff) 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 – Ms S. Butt

**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.

## Designated Safeguarding Lead – Mr S. Miah

**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
    - 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.
- 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.

## Governing Body, led by Online Safety / Safeguarding Link Governor – Mr A. Raouf

**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."

## PSHE / RSHE Lead/s – Ms. U. Sultan

**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 – Ms. Z. Navlakhi Ahmed

**Key responsibilities:**

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

## Subject / aspect leaders

**Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in 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/ Digital Strategy and Infrastructure Leader other technical support roles – Ms. Z. Navlakhi Ahmed

**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) – LBR Representative

**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 (including tutors)

**Key responsibilities:**

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the Designated 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.