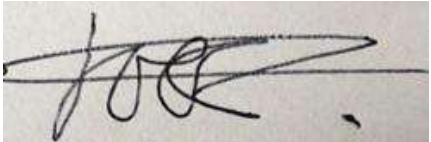




Darell Primary and Nursery School

Online Safety Policy

Governors' Committee Responsible	Full Governing Body
Status	Statutory
Review Cycle	Annual
Date written/last review	December 2025
Date of next review	December 2026
Approved By: Joe Porter Headteacher	
Approved By: Laura Morgan - Chair of Governors	

Introduction

Key people / dates

Designated Safeguarding Lead (DSL)	Emma Claridge
Deputy Designated Safeguarding Lead	Joe Porter
Link governor for safeguarding	Laura Morgan Marie Berry
Computing Lead	Olivia Durrani
Network manager	Laura Gavin

What is this policy?

Overview

This policy promotes a whole-school approach to online safety by setting expectations for online behaviour, ensuring staff understand their safeguarding roles, and maintaining high standards for digital conduct both in and out of school. It supports safe and responsible technology use while establishing procedures for handling online incidents.

Scope

The policy applies to all members of the Darell community, including staff, governors, parents, and pupils, who access digital technology or use it in their school role, whether on-site or remotely. As such this is a detailed policy and so for ease of use please see the two page summary below and then the contents page for specific information and suggested audience for that information:

Summary of LGfL Online Safety Policy 2025

1. **Introduction** Online safety is integral to safeguarding and requires a whole-school approach. This policy aligns with statutory guidelines, including 'Keeping Children Safe in Education 2024' and 'Teaching Online Safety in Schools.' It complements the school's Child Protection & Safeguarding Policy.
2. **Key Personnel**
 - **Designated Safeguarding Lead (DSL):** Emma Claridge
 - **Deputy DSL:** Joe Porter
 - **Safeguarding Link Governor:** Laura Morgan, Marie Berry
 - **Computing Lead:** Olivia Durrani
 - **Network Manager:** Laura Gavin
 - **Add DPO here?**
 - IT service provider – Click on it?
3. **Policy Review & Communication** The policy is reviewed annually and updated as necessary. It is accessible via the school website, included in staff induction, and discussed in training sessions and parent workshops.
4. **Main Online Safety Risks (2023/2024)**
 - Inappropriate use of **WhatsApp and gaming platforms** with chat features.
 - **AI-generated content risks**, including misinformation and explicit deepfake material.
 - **Children's increased screen time** (average 3 hours/day) and exposure to social media.
 - **Cybersecurity threats**, with 52% of primary schools experiencing breaches.
 - **Extremism and misinformation**, including false narratives leading to real-world violence.
 - **Social media misuse**, including unauthorised filming of school staff and pupils.
5. **Roles & Responsibilities**
 - **DSL:** Oversees online safety, filtering, and monitoring systems.

- **School Staff:** Monitor online activities, educate pupils, and report concerns.
- **Governors:** Provide strategic oversight and ensure compliance.
- **Parents & Carers:** Encourage responsible online behaviour and adhere to the parental Acceptable Use Policy (AUP).

6. Online Safety Education The curriculum integrates online safety across subjects, particularly **PSHE, Computing, and Citizenship**. Topics include:

- Recognising and responding to online risks.
- Developing critical thinking to combat misinformation.
- Understanding privacy, security, and digital footprints.
- Addressing issues such as cyberbullying and the responsible use of AI.

7. Safeguarding & Reporting Procedures All online safety concerns are treated as safeguarding issues. Staff report concerns to the DSL using **CPOMS**. The school liaises with agencies such as the **UK Safer Internet Centre, Police, and Prevent Officers** where necessary.

8. Managing Online Incidents

- **Sharing of Nudes:** Managed per **UKCIS guidance**; staff must report incidents without viewing or sharing content.
- **Bullying & Harassment:** Cyberbullying is treated under the school's **Anti-Bullying Policy**.
- **Extremism & Radicalisation:** The school follows the **Prevent Duty** to monitor and report concerns.
- **Social Media Incidents:** Negative or harmful content posted online by parents or pupils may lead to intervention.

9. Data Protection & Cybersecurity

- Staff and pupils must use **school-approved platforms** (e.g., **Google Classroom, Arbor, CPOMS**).
- Filtering and monitoring systems are reviewed termly by **ClickOn IT London**.
- The school enforces strong **password policies, access control, and data encryption**.

10. Use of Devices & Technology

- **Personal devices** (Years 5 & 6) must be turned off and handed in at the school office
- **Staff mobile phones/Smart watches** can only be used in designated areas.
- **Social Media:** Staff and pupils must not connect via personal accounts.
- **School trips:** A **school duty phone** must be used for communications.
- **Confiscation & Search:** Devices may be searched in line with **DfE guidance**.

11. Monitoring & Review

- **Filtering & monitoring checks** occur termly.
- **Annual online safety audits** are conducted.
- **Parent communication** includes monthly newsletters and online safety workshops.

This policy ensures a safe digital environment by promoting responsible online behaviour and proactive safeguarding measures.

Contents

Subheading	Stakeholder relevance
Roles and responsibilities & Annex A	Parents & Staff & Staff Annex A
Education & curriculum	Parents
Handling safeguarding concerns and incidents	Staff & parents
Cyber security	Staff
Priority areas	Staff
Bullying	Staff and parents
Child-on-child sexual violence and sexual harassment	Staff & parents
Misuse of school technology	Staff & parents
Social media incidents	Staff & parents
Extremism	Staff
Data protection	Staff, parents & governors
Appropriate filtering and monitoring	Staff
Monitoring strategies	Staff
Messaging and communication	Staff
Behaviour and usage	Staff & parents
Use of generative AI	Staff
Online storage	Staff
School website	Staff
Digital images	Staff
Social media	Staff & parents
Device usage	Staff & parents
Annex A	Staff

Roles and Responsibilities

All school community members must act respectfully online and offline, report concerns, and use technology responsibly. Specific roles and responsibilities are detailed in Annex A, with all staff required to read the general section.

Education and Curriculum

Darell School integrates online safety into its curriculum to ensure pupils develop digital competencies. Online safety is embedded in subjects like RSHE, Computing, and Citizenship, with all staff playing a role in reinforcing it across school activities. The school follows the **Raspberry Pi Foundation framework** and conducts annual curriculum reviews and online safety audits. Parents receive regular updates through newsletters, the school website, and planned lessons.

Handling Safeguarding Concerns and Incidents

Online safety is part of safeguarding, and concerns must be reported to the **Designated Safeguarding Lead (DSL)** via CPOMs. Reports of staff misuse go to the Headteacher or Clerk to governors if relation to Headteacher. The school collaborates with external agencies like the **UK Safer Internet Centre** and **Prevent Officers**. Parents and authorities are informed when necessary.

Cyber Security

The school takes precautions to safeguard pupils online but acknowledges external risks. It encourages prompt reporting of incidents and ensures sustainable reporting procedures during school closures.

Priority Areas

- **Nudes – Sharing Nudes and Semi-Nudes**

Staff must follow **UKCIS guidance** and report incidents to the DSL without viewing or sharing images. The school prioritises support over criminalisation for affected pupils.

- **Upskirting**

Upskirting is a criminal offence and a form of sexual harassment. Pupils are encouraged to report any concerns to staff.

Bullying

Online bullying (cyberbullying), including incidents outside school, should be handled like any other form of bullying, following the school's **bullying policy**. This includes issues related to banter. Staff should be aware that fights may be filmed, live-streamed, or shared online, and fake profiles can be used to harass children. Resources for teaching about bullying are available at **bullying.lgfl.net**.

Child-on-Child Sexual Violence and Sexual Harassment

Any incidents of sexual harassment or violence, online or offline, must be reported to the **Designated Safeguarding Lead (DSL)**, who will follow **Keeping Children Safe in Education (KCSIE) guidelines**. Staff should foster a **zero-tolerance culture** and recognise that inappropriate behaviours should not be dismissed as 'low level'. This could include actions such as bra-strap flicking and careless language (although this list is not exhaustive), which will be covered in staff training.

Misuse of School Technology

Clear rules govern the use of school technology, including **devices, networks, cloud platforms, and social media**, both on and off-site. These are outlined in the **Acceptable Use Policy** and this document.

- Pupils who break these rules will face consequences under the **behaviour policy**.
- Staff who breach them will be subject to actions outlined in the **staff code of conduct**.
- The school reserves the right to **restrict or withdraw** access to technology or permission to bring personal devices on-site.

Social Media Incidents

Social media incidents involving pupils are often **safeguarding concerns** and must be handled accordingly, following the **safeguarding policy** and related policies (e.g., **Acceptable Use Policy, Social Media Policy, Home-School Agreement**).

- Breaches will be dealt with under the **behaviour policy** (for pupils) or the **staff code of conduct**.
- If an inappropriate or harmful post is made by a school community member (e.g., parent or visitor), the school will contact the person making the post and **request its immediate removal**.
- If a third party makes the post, the school may **report it to the platform** and seek support from the **Professionals' Online Safety Helpline (POSH)**.

Extremism

The school adheres to the **Prevent Duty** and has strict obligations regarding **radicalisation and extremism**.

- Staff must not support or promote extremist views, individuals, or organisations.
- Extremist content **must not be accessed, shared, or downloaded** on school systems.
- Parents are encouraged to help monitor and prevent exposure to extremist content, especially on **social media**.

Data Protection and Cyber Security

All **pupils, staff, governors, volunteers, contractors, and parents** must follow the school's **Data Protection and Cyber Security Policy**. Effective **data protection and cyber security** are essential for safeguarding children, as highlighted in **Keeping Children Safe in Education (KCSIE)** and the **DfE Standards of Cyber Security for Schools and Colleges**.

- **Sharing information to protect children:** Data protection laws **do not prevent** sharing information if it is necessary for safeguarding. Schools **do not usually need consent** to share personal information when protecting a child's welfare.

Appropriate Filtering and Monitoring

The **Designated Safeguarding Lead (DSL)**, oversees **filtering and monitoring** in collaboration with the schools IT provider, ensuring compliance with **DfE standards**:

- **Roles and responsibilities** are clearly assigned.
- **Filtering and monitoring provisions** are reviewed **annually**.
- Harmful content is **blocked** while ensuring effective teaching and learning.
- **Monitoring strategies** are in place to meet safeguarding needs.

Staff are trained to recognise **potential risks** and **over blocking**. They can report concerns via the **IT Provider helpdesk** and will provide feedback during regular checks.

- **Filtering reports** are reviewed **half-termly** by the DSL, with appropriate actions taken.
- **Half-termly system checks** and an **annual online safety audit** are conducted.
- **SafeSearch** is enforced on all devices, and **YouTube is set to LGFL School Protect mode**.
- **Out-of-hours policies** apply only to staff, as pupils no longer take devices home.

Monitoring Strategies

DfE standards outline different **monitoring strategies** to **minimise risks** on internet-connected devices, including:

- **Physical monitoring** (staff watching screens).
- **Live supervision** (device management software).
- **Network monitoring** (internet traffic and web access logs).
- **Device monitoring** (software or third-party services).

At Darell, the IT service provider holds **admin rights** to all school devices, ensuring **staff cannot** install applications or change system settings.

Messaging and Commenting Systems

Authorised Communication Systems

- **Pupils** communicate via **Google Classroom**.
- **Staff** use **LGFL email** for school-related emails and are **not permitted** to use personal accounts.
- **Staff communicate with parents** via **Arbor text messages and in-app messaging** or from the parents@ email address

All communication systems are **centrally managed** to protect **privacy, security, and safeguarding best practice**. Any **new platform or app** requiring **child logins or storing school data** must be **approved** and centrally managed.

Unauthorised Use and Mistakes

- **Using unauthorised systems** may be a **safeguarding or disciplinary issue** and must be reported to the **DSL (for pupils)** or the **Headteacher (for staff)**.
- If **data is mistakenly sent from a private account**, the **DSL and the Headteacher** must be informed immediately. The headteacher may consider informing the Data Protection Officer (DPO)

Behaviour and Usage Principles of Messaging/Commenting Systems

Further details on the points below are outlined 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 required at all times. Messaging systems must not be used to send **bullying, aggressive, rude, insulting, illegal, or otherwise inappropriate messages**. Staff must also avoid actions that could bring the school into **disrepute** or compromise their **professionalism**.
- **Data protection principles** apply to all school communications in line with the **Data Protection Policy**. Staff must use **authorised systems only**.

- **Staff personal use of email** is allowed but must be **reasonable** (not excessive, not during lessons). **All use is monitored**, and emails containing inappropriate language, images, malware, or links to adult sites **may be blocked** and handled according to school policy.

Use of Generative AI

Darell recognises the growing use of **generative AI** tools (e.g. **ChatGPT, Bard, Co-Pilot, Adobe Firefly**) and follows **DfE guidance**:

- Discussions with pupils on AI use take place.
- Pupils may encounter AI-generated content at home, which can have both **positive (creativity, learning)** and **negative (misinformation, deepfakes, bullying, inappropriate content)** impacts.
- Staff have an **open dialogue** about AI's role in reducing teacher workload, and the school is currently **trialling "Teachmate AI"**.
- The **trial's benefits and risks** will be reviewed before making any decisions on future AI use.

Online Storage and Learning Platforms

The **same principles** of appropriate behaviour, **data protection**, and **cyber security** apply to **online storage and learning platforms**. At Darell, these include:

- **Google Drive, CPOMs, Renaissance, and Arbor.**
- Any **new platforms** must be **approved** by **Headteacher or DSL** before use.

School Website

The school website serves as a **public-facing information portal** with **significant reputational value**.

- **School Business Manager** is responsible for **content updates and compliance** with **DfE regulations**, under the delegation of the **Headteacher and Governors**.
- The website is **managed by Juniper**.
- **Copyright laws must be followed** when submitting content. Schools can be fined for **copyright breaches**, so staff must ensure that materials are used with **proper permissions**.
- **Open-access libraries** of images, sounds, and other media should be used instead of unverified content from **Google or YouTube**. If uncertain, staff should check with the Network Manager.

Digital Images and Video

- **Parental Consent**: When a pupil joins the school, parents/carers provide consent on how their child's image may be used (e.g. displays, newsletters, marketing, websites, social media). **Internal assessment does not require express consent**.
- **Usage Checks**: Staff must check the latest **consent database** before using any photo or video. Public facing materials never include a pupil's **full name**.
- **Staff Guidelines**: Staff **must not** use personal devices for capturing images/videos. Usage follows the **Acceptable Use Policy** and contract terms.
- **Storage and Monitoring**: Photos are stored on the **school server** per the **Data Protection Policies retention schedule**. **DSL** reviews school device images **half-termly**, and any concerns follow **safeguarding procedures**.

- **Privacy and Safety:** Parents and staff are reminded **not to share images on social media** without permission, as this could pose risks related to **child protection, data protection, and personal privacy**.
- **Online Safety Education:** Pupils learn about **image manipulation**, considering **audience appropriateness**, and the importance of **privacy settings** when sharing images online. They are taught **not to post images/videos of others without permission** and how to handle **cyberbullying or privacy breaches**.

Social Media

Our Social Media Presence

Darell actively manages its **online reputation**, as school perception online has wide implications

- **The Headteacher and the School Business Manager** manage the school's **Instagram and Facebook accounts** and monitor **Wikipedia, Google reviews, and online mentions**.
- The school responds to **praise and criticism responsibly** to maintain a **positive reputation**.
- Is commenting on social media posts (facebook/instagram turned off?)

Staff, Pupils' and Parents' Social Media Use

- **Expected Behaviour:** Social media conduct must be **respectful and appropriate**, mirroring **face-to-face** interactions. Posts must not be **bullying, aggressive, rude, illegal, or damaging to the school's reputation**.
- **Raising Concerns:** If parents have **concerns**, they should **contact the school directly** rather than posting on social media. Complaints should follow the **school's official complaints procedure**.
- **Age Restrictions:** Many platforms have a **minimum age of 13**, yet issues often arise from underage pupil use. Parents are encouraged to **enforce age restrictions** while supporting their children's **online safety education**.
- **Online Safety Lessons:** Pupils learn about **social media behaviour, online friendships, privacy settings, and reporting issues**. Adult role models play a crucial role in shaping pupils' online conduct.
- **Parental Support:** Parents are advised to discuss **apps, sites, and games** with their children, focusing on **screen time, safety, and appropriate usage**. The **Digital Family Agreement** and **Children's Commission Digital 5 A Day** offer useful guidance.

School Communication Policy

- The school's **Instagram account** handles general enquiries, but parents must **not** use it for individual concerns.
- **Email** is the **official communication channel** between parents and the school. This should be via the **parents@** email address
- **Social media, including WhatsApp, is not appropriate for school-related communication**.

Social Media and Staff Conduct

- **Staff and pupils (including former pupils) must not connect on social media**. Pupils should not send **friend requests** to staff, and staff must **not follow pupil accounts**.
 - **Exceptions** (e.g. family links) must be **approved by the Headteacher**.
- Staff must **uphold the school's reputation** by **maintaining strict privacy settings** and avoiding **inappropriate content** online.
- Staff must not **discuss the school or its stakeholders** on social media.
- **Professional Consequences:** The **Teacher Regulation Agency** has issued **Prohibition Orders** due to **misuse of social media** by staff.

Respecting Privacy on Social Media

- **Permission is required before sharing images/videos of others.**
- **Parents must not film or record** interactions with pupils or staff without consent.
- Sharing **other children's images** on social media is **prohibited** due to **privacy and safety risks**.
- The school may use images for **internal assessment**, but **public sharing only occurs with parental consent**.

Device Usage

Acceptable Use Policy (AUP)

- School devices must be used in accordance with **AUP rules**, including when used at home.
- Policies on **copyright, data protection, social media, technology misuse, and digital images** apply to device usage.

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

- **Year 5 & 6 pupils** may bring mobile phones if they **walk to and from school alone**. Phones must be **turned off, handed in at the office** on arrival, and collected at the end of the day.
- **Staff** must keep phones and smart watches on **silent** and use them **only in private staff areas** during school hours. Personal data must **never** be downloaded onto a private phone. Urgent calls should go through the **school office**.
- **Medical Monitoring Apps**: Parents must sign an **appropriate use policy** for devices used for medical monitoring.
- **Volunteers, contractors, and governors** must **not** use phones in the presence of children. If photography is required (e.g. for building maintenance), **Headteacher approval** is needed, and a **staff member must be present**.
- **Parents** should keep phones **off and in pockets** while on-site and seek **permission before taking photos**. Calls to pupils during the school day should go **via the school office**.
- **BYOD users** (staff or students) must **not** use mobile hotspots as this could **bypass the school's internet filtering**. How would this be enforced? By the AUP policy?

Use of School Devices

- Staff and pupils must follow the **AUP** when using school devices **on-site or at home**.
- Devices must not be used in ways that breach the **AUP, behaviour policy, or staff code of conduct**.
- **Wi-Fi access** is available for **school-related and limited personal use** under AUP guidelines and is **monitored**.
- School devices are **restricted** to **pre-installed** apps/software.
- **All usage** of devices, systems, and platforms may be **tracked**.

Trips and Events Away from School

- Teachers are issued a **school duty phone** for communication with parents during trips.
- If a **personal phone** is used in an emergency, the **number must be hidden** to protect privacy.
- Any **deviation from this policy** must be reported to the **Headteacher immediately**.

Searching and Confiscation

- The **Headteacher and Designated Safeguarding Lead (DSL)** have statutory authority to **search pupils' property**, including mobile phones, if there is **reasonable suspicion** of **inappropriate or illegal content** (e.g. sexual images, violence, bullying).
- Wherever possible, searches at Darell will be conducted **with the child's and parents' permission**. Pupils will be asked to **show the content voluntarily**. Parents may be requested to **provide screenshots** as evidence.
- Full details on **search procedures** can be found in the school **Behaviour Policy**: [Behaviour Policy](#).

Appendix – Roles

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

All school staff must read the "All Staff" section as well as any other relevant to specialist roles.

Roles:

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

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook

<https://www.darell.richmond.sch.uk/page/?title=Policies&pid=380> 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 safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2024) 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 over blocking, 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

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 undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the 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 safeguard.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of 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.
- 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 organisation.
- Ensure that ALL governors and undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.”
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- 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.
- Promote an 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 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

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.
- 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.
- 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 Lead

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."
- 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 and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- Note that an RSE 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 RSHEI 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 / 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/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 [e.g. [schoolprotect.lgfl.net](https://www.schoolprotect.lgfl.net) and [monitoring.lgfl.net](https://www.monitoring.lgfl.net)]. 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.
- 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 / delete this reference as I think it is the same as DSL/ data protection officer / LGfL nominated contact – who is this Headteacher? / 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 students 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.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer (DPO)

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the Data Protection and cyber security 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 pupil is aged 25 or older)'. However, some local authorities require record retention until 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 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 pupil home-school agreement

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 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.