




We are friends journeying with Jesus in faith, hope and trust as we live, love and learn together

Online Safety Policy

September 2025

Introduction

 Emmaus Church of England and Catholic Primary School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Alan Williams
	Deputy Designated Safeguarding Leads / DSL Team Members	Alan Williams, Carol Yates and Chris McGivern
	Link governor for safeguarding	Kath Nelson
	Link governor for webfiltering	Kath Nelson
	Curriculum leads with relevance to online safeguarding and their role	Sarah Hogben – Computing Lead
	Network manager / other technical support	Computeam
	Date this policy was reviewed and by whom	1.9.24
	Date of next review and by whom	1.9.25

Purpose of this Policy

Online safety is a vital part of safeguarding at Emmaus and must be addressed through a **whole-school approach**. This policy complements our statutory **Child Protection & Safeguarding Policy** and is aligned with:

- *Keeping Children Safe in Education (KCSIE) 2025*
- *Teaching Online Safety in Schools*
- Statutory RSHE guidance

It applies across all subjects and is designed to protect pupils, staff, and the wider school community in both **online and offline contexts**.

All online safety concerns must follow our **safeguarding reporting procedures**.

Policy Ownership and Review

This policy is reviewed **annually**, with updates made throughout the year as needed (e.g. due to legislative changes such as the Online Safety Bill). It is shaped collaboratively with input from:

- Senior Leaders
- Governors
- Staff
- Parents
- Pupils

Changes to the policy or related Acceptable Use Policies (AUPs) will be communicated **promptly and clearly** to all stakeholders.

Leadership and Responsibility

The **Designated Safeguarding Lead (DSL)** has overall responsibility for online safety, in line with KCSIE. Other staff, including RSHE and Computing leads, support the curriculum aspect, but all members of staff have a role in **modeling safe behaviour, raising concerns, and supporting pupils**.

While tasks may be delegated, **accountability remains with the DSL**.

Current Online Safety Risks (2025–2026)

We remain alert to emerging online risks affecting children and young people, including:

- **AI Tools** (e.g. ChatGPT, image generators): Potential for misuse, age-inappropriate content, and plagiarism.
- **Increased Screen Time**: Linked to cost-of-living challenges and fewer offline activities.
- **Social Media Exposure**: High use of YouTube, WhatsApp, TikTok, and Snapchat among pupils (despite age restrictions).
- **Early Mobile Use**: 20% of 3–4 year olds have their own phones; this rises to over 90% by end of primary school.
- **Online Child Exploitation**: A significant rise in *self-generated* sexual abuse imagery among 7–10 year olds (IWF report).

We are committed to **educating pupils and families** to navigate these risks and ensuring our technical and curriculum strategies reflect them.

Communication and Accessibility

This policy will be shared:

- On the school website
- In staff induction packs
- During annual safeguarding training
- Alongside Acceptable Use Policies (for pupils, staff, parents, governors, contractors)

Acceptable Use Agreements are reviewed and reissued **annually** or as needed.

Aims of the Policy

Our online safety policy aims to:

- Establish clear expectations for **digital conduct and online behaviour**
 - Promote safe, respectful, and responsible technology use
 - Support staff in protecting themselves and pupils from risk
 - Reinforce that **online behaviour is subject to the same standards** as offline conduct
 - Provide a framework for **responding to incidents**
 - Encourage collaboration between **curriculum, safeguarding, and IT teams**
 - Prepare pupils to **safely engage in the digital world**
-

Scope

This policy applies to all members of the Emmaus community:

- Pupils
- Staff (including supply and support staff)
- Governors
- Parents and carers
- Contractors
- Volunteers
- Visitors

It applies to use of school systems both **on-site and remotely**, and to **all technology used in a school context**.

Roles and Responsibilities

Everyone in our school shares responsibility for online safety.

Refer to **Annex A** of the full policy for detailed role descriptors, including:

- All Staff
- Pupils
- Parents
- Governors
- Curriculum Leads (e.g. RSHE, Computing)
- Technical Support Teams

All staff must understand:

- The school's **filtering and monitoring systems**
 - Their role in supervising safe digital use
 - The importance of **timely reporting**
-

Online Safety in the Curriculum

Online safety is taught through a **whole-school approach**, with key links in:

- **Computing**
- **PSHE/RSHE**
- **Citizenship**

We embed online safety in all subject areas and address real-life digital issues including:

- Misinformation and fake news
- Privacy and data protection
- Cyberbullying
- Online relationships and consent
- Copyright and digital ownership

Resources to support this approach are available via:

- safetraining.lgfl.net
- saferesources.lgfl.net

Supervision and Safe Use

Staff must **actively supervise** any use of technology by pupils and be aware of:

- Age-appropriate content
- Approved platforms and filtering systems
- Children’s digital literacy and potential vulnerabilities

Parents are informed of the **tools and platforms** their children use and are encouraged to monitor use at home.

Responding to Concerns and Incidents

Online safety concerns must be treated as **safeguarding issues**. Staff should:

- Report incidents to the **DSL or online safety lead** immediately (same day).
- Follow the school's **escalation procedures**.
- Use professional judgement to identify **patterns or context** where pupils may be at risk.

Any concern about staff misuse must be reported directly to the **Headteacher** or, if about the Headteacher, to the **Chair of Governors** and the **Local Authority Designated Officer (LADO)**.

Where necessary, we involve external agencies including:

- CEOP
- IWF
- LGfL POSH helpline
- Police
- LA safeguarding teams

We also commit to informing parents and, where appropriate, the Police in serious cases such as **sexting, upskirting, or harmful sexual behaviour**.

Relevant linked policies include:

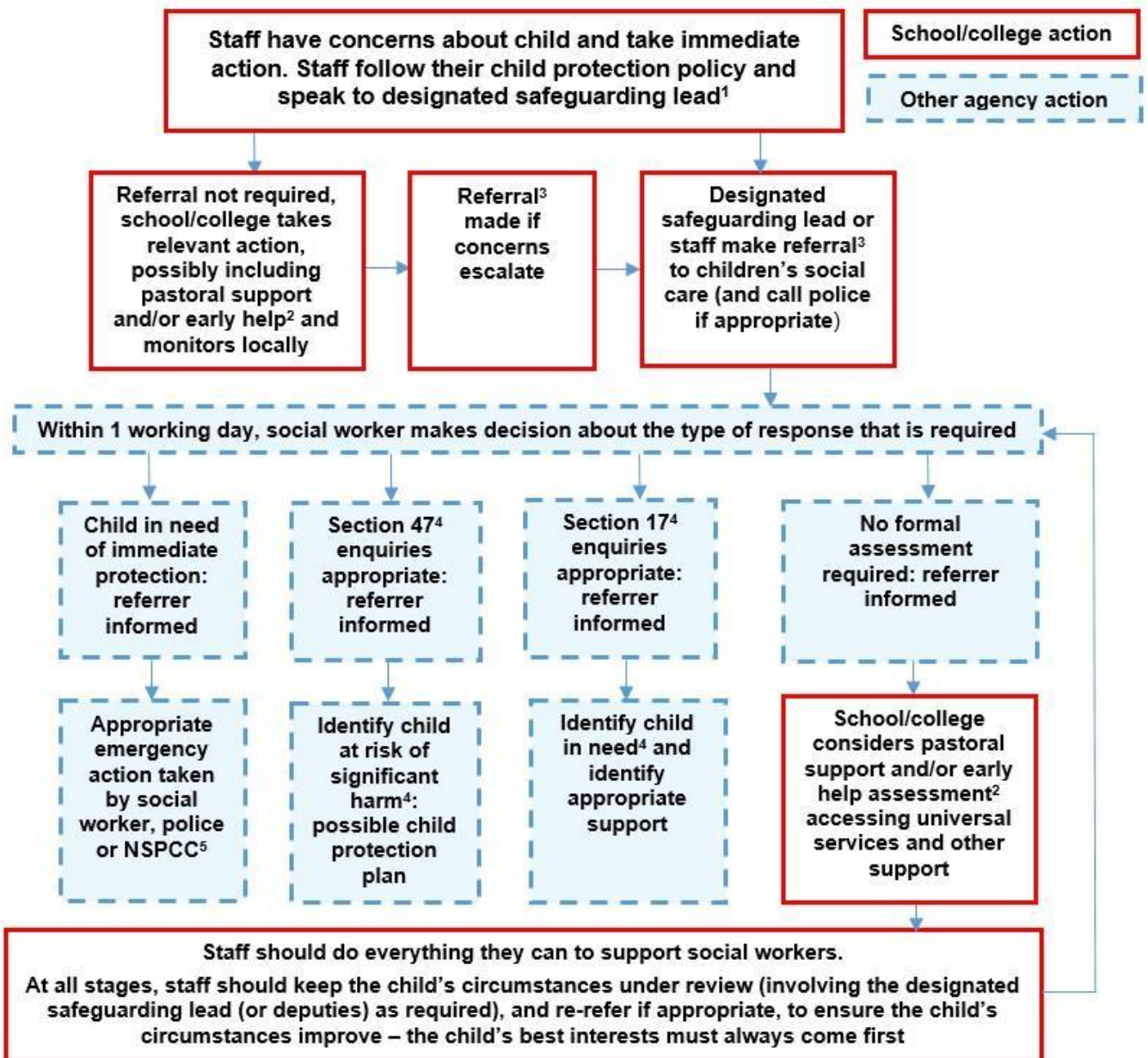
- Safeguarding & Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policies
- Data Protection and Privacy Policies

Reporting and Support

Concerns should follow internal channels first. The DSL is responsible for all referrals to MASH or relevant external agencies.

Additional resources:

- **reporting.lgfl.net** – external helplines for pupils and staff
- **UK Safer Internet Centre** – professionals’ helpline
- **NSPCC** – Report Abuse in Education helpline
- **Prevent / Terrorism / Fraud / Hate crime** hotlines
- Anonymous support lines for young people



Sexting – Sharing nudes and semi-nudes

Sharing Nudes and Semi-Nudes (Previously Known as Sexting)

All schools, regardless of phase, should follow the **UK Council for Internet Safety (UKCIS)** guidance: [Sharing nudes and semi-nudes: advice for education settings](#) which aims to avoid the unnecessary criminalisation of children and young people.

⚠ Important: If one of the individuals involved is aged 18 or over and the other is under 18, this is **not** considered ‘sexting’ but constitutes **child sexual abuse** and must be treated as such.

What Staff Should Know and Do

A **one-page summary document** — [Sharing nudes and semi-nudes: how to respond to an incident](#) — is available and **must be read by all staff**, not just those in teaching or DSL roles.

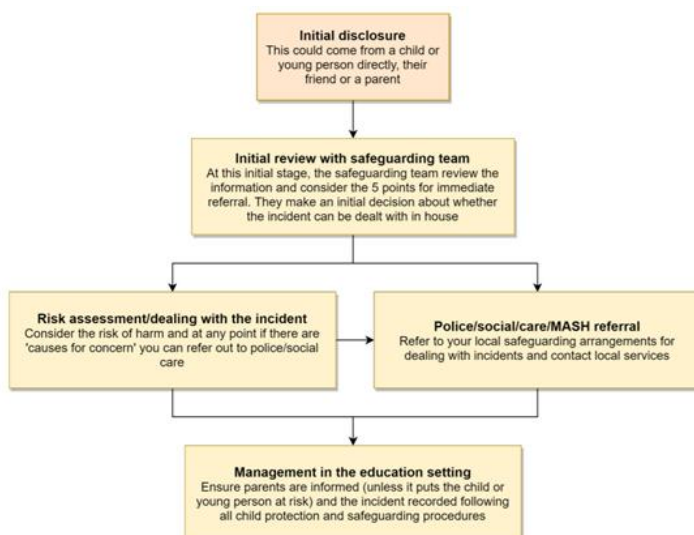
This is because it is often **non-safeguarding staff** who first become aware of an incident, and **immediate and appropriate action is essential**.

Staff must NOT:

- View
- Share
- Copy
- Delete
- Forward
- Ask anyone else to do any of the above

Instead, staff must **report the incident directly and immediately** to the Designated Safeguarding Lead (DSL), who will handle it in line with national guidance.

The DSL will use the **full UKCIS guidance document** to assess the situation and decide the next steps and whether a referral to external agencies (e.g. police, social care) is necessary



Immediate Referral: 5 Criteria

The following five situations **require immediate referral to external agencies** as outlined in the UKCIS guidance:

1. **Involvement of an adult** (someone aged 18 or over)
 2. **Coercion, blackmail, or grooming**, or if the child is unable to give informed consent (e.g. due to SEND)
 3. **Sexual acts depicted** are violent or developmentally inappropriate
 4. **Any individual shown is under 13 years old**
 5. **The child is at immediate risk of harm**, e.g. suicidal thoughts or self-harming related to the incident
-

Creating a Supportive Culture

It is essential that all students understand:

- **While sharing nudes is illegal**, they can always **speak to a trusted adult** if they are worried or have made a mistake.
- Staff will support and guide them and not jump to criminalise them.

The UKCIS guidance and materials to support classroom teaching about this issue are available at:

 sexting.lgfl.net

Upskirting

Upskirting—taking images under someone’s clothing without their knowledge or consent—is a criminal offence and a serious form of sexual harassment, as defined in *Keeping Children Safe in Education (KCSIE)*. Pupils who experience or have made mistakes in this area are encouraged to speak to a member of staff without fear of judgment.

Bullying (Including Online Bullying)

All bullying, including online or cyberbullying (even if it occurs offsite or at home), will be addressed using the school's anti-bullying policy. Increasingly, reports include:

- Fights being recorded and shared online.
- Fake profiles used to impersonate and harass others.

Staff are reminded to remain vigilant and use available DfE resources and case studies for guidance: bullying.lgfl.net.

Child-on-Child Sexual Violence and Harassment

Section 5 of *KCSIE* outlines the expectations for handling incidents of sexual violence or harassment between children. All staff should:

- Maintain a zero-tolerance approach.
- Understand that harmful behaviours exist on a continuum.
- Avoid minimising behaviours like bra-strap flicking or inappropriate language.

All incidents, whether online or in person, must be reported to the Designated Safeguarding Lead (DSL). Staff should assume “it could happen here” and act accordingly. The recent rise in online misogynistic content is a key concern and should be actively addressed.

Misuse of School Technology

All technology usage by pupils and staff must follow the Acceptable Use Policy (AUP). This includes school devices, internet access, platforms, and Bring Your Own Device (BYOD) guidelines. Misuse will be addressed via:

- The behaviour policy (pupils)
- The staff code of conduct (staff)

Reminders will be given at the start of the year and during any periods of remote learning. The school may revoke access to technology if necessary.

Social Media Incidents

Expectations for online conduct are outlined in the school's social media and AUP policies. Breaches will result in disciplinary action:

- Pupils: Behaviour policy
- Staff: Code of conduct

Inappropriate content must be promptly removed upon request. If third-party content affects the school community, the school may escalate the issue to the platform or seek help from the Professionals' Online Safety Helpline (POSH).

Data Protection and Cybersecurity

All members of the school community—including staff, pupils, governors, volunteers, contractors, and parents—must follow the school’s data protection and cybersecurity policies.

Key points include:

- Safeguarding takes precedence over data-sharing concerns.
- Consent is not typically needed when sharing data to protect a child.
- The Data Protection Act 2018 and UK GDPR do not prevent essential information-sharing for safeguarding.

KCSIE now references the DfE Cybersecurity Standards (since 2023).

Appropriate Filtering and Monitoring

Schools must implement appropriate filtering and monitoring systems that:

- Protect children from harmful content.
- Avoid excessive restrictions that hinder learning.

As per *KCSIE 2023*, the DSL now has primary responsibility for these systems.

DfE Filtering & Monitoring Standards require schools to:

- Assign clear roles/responsibilities for system management.
- Review systems annually.
- Prevent harmful content while supporting teaching.
- Implement robust monitoring strategies.

Monitoring strategies may include:

- Staff supervision of screens
 - Device management software
 - Network-level log file reviews
 - Device monitoring tools
-

Emmaus School Approach:

- **Filtering Provider:** LGfL (on site and for school devices at home)
- **Management:** Safeguarding Team
- **Oversight:** DSL with SLT support
- **Technical Support:** Computeam
- **Check Frequency:** Half-termly by Computeam
- **Annual Review:** Conducted as part of the Online Safety Audit (onlinesafetyaudit.lgfl.net)
- **System Guidance:** Available at appropriate.lgfl.net

All staff must be informed of their responsibilities and report:

- Overblocking issues
- System workarounds by students
- Concerns about monitoring or filtering gaps

Training and induction will reinforce these duties at the start of each academic year and throughout as needed.

Messaging and Communication Systems

Authorised Platforms

- Pupils communicate with each other and staff using **Purple Mash**.
- Staff use **Outlook email** for all school communication. Personal email accounts or other messaging platforms must never be used for school business, including communication with pupils, parents, or colleagues where school/child data is involved.
- Staff may use **ParentPay** and **ParentApp** to communicate with parents.

All authorised systems are centrally managed and administered by the school or an approved IT partner. This ensures communications can be monitored and audited if necessary, safeguarding staff, pupils, and parents in line with UK data protection legislation.

Use of any new communication or data platform must be approved in advance by the Headteacher and managed centrally. Unauthorised use may be treated as a safeguarding concern or disciplinary matter and must be reported to the **DSL** (if involving a child) or the **Headteacher** (if involving a staff member).

If a private account is accidentally used to send or store school-related data, the **DSL, Headteacher or DPO** (as appropriate) must be informed immediately.

Behaviour and Usage Principles

- Full guidance is available in the school’s **Social Media Policy, Acceptable Use Agreements, Behaviour Policy, and Staff Code of Conduct.**
 - All communication must be respectful and appropriate. Inappropriate, offensive, bullying, aggressive, or illegal content is strictly prohibited. Staff must avoid any behaviour that could bring the school into disrepute.
 - Data protection principles must always be followed, in line with the school’s **Data Protection Policy.**
 - Limited personal use of email is permitted, provided it is reasonable, does not disrupt lessons, and complies with behaviour expectations. All email use is monitored and subject to filtering; inappropriate content may be blocked and investigated.
-

Online Storage and Learning Platforms

The same principles apply to any online system used for storing files, teaching, or collaboration. Data protection and cybersecurity must be prioritised at all times, in line with the school’s **Cybersecurity and Data Protection Policy.**

School Website

The website is a key public information channel with reputational importance. Day-to-day content management is delegated to staff, under oversight of the Headteacher and Governors. The site is managed by **Juniper Education.**

Staff must:

- Ensure compliance with copyright law when submitting materials.
 - Use open-access or licensed resources and always credit sources.
 - Avoid assuming online content (e.g. from Google or YouTube) is free to use.
-

Digital Images and Video

Parental consent for image use is collected at admission and applies to:

- Displays within school
- Newsletters
- Paper-based marketing
- Website or prospectus
- Social media
- Specific high-profile projects

Staff must check the consent database before using any image. Public-facing images identify pupils only by first name.

Photos/videos may only be taken in line with the **Acceptable Use Policy**:

- Personal devices may be used only when appropriate, transparently, never in one-to-one situations, and files must be transferred promptly to school storage and deleted from personal/cloud accounts.
- Images are stored securely according to the school's retention schedule.

Parents and staff are reminded annually not to share photos/videos without permission, for safeguarding, cultural, or privacy reasons. Pupils are taught about digital footprints, consent, and the risks of sharing images online.

Social Media

School Presence

The school actively manages its online reputation (e.g. social media accounts, reviews, Wikipedia entries). The **SLT** is responsible for official accounts and monitoring online references.

Staff, Parent, and Pupil Use

- All school community members are expected to behave respectfully online, as they would face to face.
- Negative, bullying, aggressive, or defamatory posts are not acceptable, even in private groups.
- Concerns about the school should be raised directly with staff or through the complaints procedure—not via social media.
- Pupils must not 'friend' or connect with staff, governors, volunteers, or contractors. Staff must not follow or engage with pupil accounts. Exceptions for family links must be declared and approved by the Headteacher.
- Staff should maintain strict privacy settings and avoid any posting that could bring the profession or school into disrepute.

Parents are encouraged to discuss social media use with their children and respect platform age restrictions (13+ in most cases, 16+ for WhatsApp).

Device Usage

Personal Devices

- **Pupils (Years 5–6):** May bring mobile phones only if walking home alone. Phones must be handed to the class teacher on arrival. Misuse will result in withdrawal of privileges.
- **Staff:** Phones must remain on silent and be used only in staff areas. Important calls during lessons require Headteacher permission. No child/staff data may be stored on personal devices.
- **Volunteers/Contractors/Governors:** Phones must remain off in the presence of children. Any required use (e.g. site photos) must be approved by the Headteacher and supervised by staff.
- **Parents:** Phones should not be used on site. Permission must be sought before photographing displays or events, and they must avoid capturing other children. Urgent messages should go via the school office.

School Devices

- Staff and pupils must follow Acceptable Use Policies.
- Devices may only run apps/software installed by the school.
- Internet/Wi-Fi is provided for schoolwork and limited personal use, subject to monitoring.
- All use of devices and systems may be tracked.

Trips and Events

In emergencies, teachers using personal phones must withhold their number to protect privacy.

Searching and Confiscation

In line with DfE guidance, the Headteacher (and authorised staff) may search pupils or devices where there is reasonable suspicion of illegal or inappropriate content (e.g. sexual images, pornography, violence, bullying).

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 must:

- Sign and follow the **Staff Acceptable Use Policy (AUP)** alongside the school’s Safeguarding Policy, Code of Conduct, and relevant sections of *Keeping Children Safe in Education (KCSIE)*.
- Report any concerns, however minor, to the Designated Safeguarding Lead (DSL).
- Keep up to date with online safety issues and guidance (e.g. KCSIE).
- Model safe, responsible, and professional behaviour when using technology both in and outside school.
- Avoid using scaring or victim-blaming language when discussing safeguarding issues.
- Support new DfE standards on filtering and monitoring by flagging problems such as over-blocking, gaps in provision, or pupils bypassing protections.

Headteacher/Principal – Alan Williams

The Headteacher is responsible for embedding online safety into whole-school safeguarding by:

- Promoting a culture of safeguarding and ensuring DSL and technical colleagues complete an online safety audit in line with KCSIE.
- Completing safeguarding training (offline and online) and ensuring all staff and governors do the same, including updates.
- Implementing safe ICT systems (filtering, monitoring, protected email) with child-safety as the priority.

- Regularly reviewing filtering/monitoring systems with DSL and technical staff; appointing a filtering and monitoring governor.
 - Overseeing remote learning safeguards and home-use protections.
 - Taking overall responsibility for information security and working with the DPO to ensure compliant but safeguarding-led data management.
 - Ensuring staff understand what to do in the event of a serious incident.
 - Overseeing safeguarding risk assessments, curriculum needs, and statutory website compliance.
-

Designated Safeguarding Lead / Online Safety Lead – Claire Creer

The DSL holds lead responsibility for safeguarding (including online) and must:

- Ensure a whole-school approach to online safety.
 - Lead on filtering and monitoring processes, working with SLT, technical staff, and governors.
 - Ensure all staff receive safeguarding training (including filtering/monitoring) at induction and updates thereafter.
 - Cascade knowledge of risks and resources to staff, pupils, and parents.
 - Ensure governors also receive safeguarding and online safety training.
 - Monitor day-to-day safeguarding concerns, using appropriate, non-blaming language.
 - Oversee consistency in online safety across RSHE and the wider curriculum.
 - Keep up to date with online risks and undertake Prevent awareness training.
 - Update this policy and related documents regularly.
 - Promote parental engagement with online safety.
 - Ensure effective reporting and disclosure systems are available both on and off site.
 - Maintain a zero-tolerance approach to child-on-child abuse, including online bullying.
 - Ensure online tutors follow safeguarding procedures and AUPs.
-

Governing Body – Led by Online Safety / Safeguarding Link Governor – Kath Nelson

Governors provide strategic oversight by:

- Approving and reviewing the effectiveness of this policy.
- Completing safeguarding and online safety training at induction and refreshers thereafter.
- Appointing a filtering and monitoring governor.
- Ensuring all staff receive safeguarding training (including online safety and monitoring).
- Reviewing school practices with DSL and Headteacher; incorporating online safety into regular safeguarding discussions.
- Supporting parent/community engagement in online safety.
- Ensuring statutory teaching of safeguarding (including online safety) as part of the curriculum.
- Ensuring compliance with data protection and child-safety principles.

PSHE / RSHE Leads – Tracey Martin

The RSHE team must:

- Embed consent, wellbeing, healthy relationships, and online safety into the curriculum.
 - Address new risks (e.g. AI misuse, financial extortion, image sharing).
 - Teach respectful online behaviour, digital resilience, and the impact of online actions.
 - Assess pupils' progress in online safety skills using diagnostic tools (e.g. SafeSkills).
 - Ensure RSHE teaching complements Computing and other subjects, with consistent messaging across school life.
 - Maintain and publish the RSHE policy on the school website.
-

Computing Lead – Sarah Hogben

The Computing Lead must:

- Deliver the online safety element of the national Computing curriculum.
 - Work closely with RSHE and DSL to ensure a consistent whole-school approach.
 - Collaborate with technical staff to align curriculum teaching with safe ICT practices.
-

Subject Leaders

Subject leaders are expected to:

- Embed online safety opportunities within their subjects where relevant.
 - Model positive attitudes and approaches to online safety.
 - Align teaching with *Education for a Connected World* and *Teaching Online Safety in Schools*.
 - Ensure subject action plans reflect online safety objectives.
-

Network Manager / Technical Support – Computeam

Technical staff must:

- Collaborate with DSL and SLT on safeguarding decisions related to technology.
- Support compliance with new DfE filtering/monitoring standards, including annual reviews and audits.
- Maintain up-to-date documentation and ensure systems align with safeguarding priorities.
- Advise staff on the consequences of system changes (e.g. YouTube filters, file-sharing permissions).
- Detect, report, and address misuse or attempted misuse of technology.
- Manage networks/devices securely with strong password policies, encryption, backup, and disaster recovery.
- Support compliance with the Data Protection and Cybersecurity Policies.

- Ensure the school website meets DfE requirements.
-

Data Protection Officer (DPO) – Liverpool City Council

The DPO is responsible for:

- Providing expertise, training, and oversight of data protection and cybersecurity compliance.
 - Ensuring policies align with safeguarding requirements.
 - Supporting lawful and safe information-sharing for child protection purposes.
 - Advising on safeguarding record retention (minimum to age 25, subject to local authority requirements).
 - Monitoring and auditing access to safeguarding data.
-

Volunteers and Contractors (Including Tutors)

All volunteers and contractors must:

- Read, understand, and sign the AUP.
 - Report concerns immediately to the DSL.
 - Stay aware of online safety issues and guidance.
 - Model professional and safe behaviour when using technology.
 - Never arrange meetings or communicate directly with pupils without the school's prior knowledge and approval.
-

Pupils

Pupils are expected to:

- Read, understand, sign, and follow the **Pupil Acceptable Use Policy (AUP)**.
 - Act safely, responsibly, and respectfully when using technology.
 - Report any concerns or misuse immediately to a trusted adult
-

External Groups (Including Parent Associations – Friends of Emmaus)

External individuals or organisations must:

- Sign an **Acceptable Use Policy** before 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 technology use, including on social media.
- Not share images or personal details of others without consent.

- Avoid posting negative, threatening, or violent comments about staff, volunteers, governors, contractors, pupils, or other parents/carers.

Appendix A

Online Safety

Acceptable Use Policy for Early Years/Key Stage 1 Pupils

This agreement will help keep me safe online and help me to be fair to others

1. I only **USE** devices or apps, sites or games if a trusted adult says I can
2. I **THINK** before I click anything that pops up or I am not sure about
3. I **ASK** for help if I'm stuck or not sure
4. I **TELL** a trusted adult if I'm upset, worried, scared or confused
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep secrets or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I always check before **SHARING** personal information, including passwords
10. I am **KIND** and polite to everyone, in real life and online.

Online Safety

Acceptable Use Policy for Key Stage 2 Pupils

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school’s internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am a friend online*** – I won’t share anything that I know another person wouldn’t want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don’t share passwords!
5. ***I am careful what I click on*** – I don’t click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it’s not my fault if I see or someone sends me something bad*** – I won’t get in trouble, but I mustn’t share it. Instead, I will tell a trusted adult. If I make a mistake, I don’t try to hide it but ask for help.
8. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
9. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can’t be sure who they are.
10. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
11. ***I don’t do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

12. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
13. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
14. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
15. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
16. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
17. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
18. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
19. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
20. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
21. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

Appendix B

September 2025

Dear Parents

Online Safety, Photograph & Video Permission

We are currently updating our parental permissions on our pupil record system and are requesting your permission for digital images to be taken of your child in school which may be used for our school newsletter, carefully vetted publications, display, teaching purposes, social media or to record activities. This may include video footage which is also used on our school website and social media sites.

Our website and social media channels are monitored daily and content uploaded and monitored by teaching staff. Your child's name will never be attached to their online images. Please note, Instagram is private for approved followers only.

Rather than ask this at each event, I would like to be able to have permission for staff to take photographs whenever they wish i.e. a school trip, during lessons, assemblies and such.

I also enclose a copy of our school Online Safety Acceptable Use Policies (AUP) for parents and pupils for your information. I request you read the document and then complete the consent form agreeing to responsible and safe use of the internet.

Please return the completed permission slip below, along with AUP's for yourself and your child, to the school office as soon as possible.

Thank you for your assistance

Yours sincerely

A P Williams

Headteacher

Permission Slip

Photographs and Videos in School

Child's name Class

I give permission for digital images of my child to be taken in school and for it to appear on carefully selected publications.

I give permission for digital images/video footage to be taken of my child which I understand may be used on the school website.

I give permission for digital images and/or video footage to be used on social media which I understand is carefully monitored by school staff

I understand this permission will remain in place for the time my child attends Emmaus Primary School

Signed

Appendix C

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not allow children and young people to add me as a friend, nor will I add them as friends, on social networking sites
- I will not use Social Media networking sites whilst at work
- If I do use Social Media in my personal life, I must make clear that any comments (e.g. political views) are my own personal opinion
- I will not create, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring Emmaus School into disrepute
- In line with safeguarding procedures, no comments should be made with reference to the school, its staff, governors, pupils, families, any persons associated with it or events.
- I will only use a school device to take photographs or film children for school purposes. In the rare event that I need to use a personal device to do this eg on a school visit with children, I will inform the Headteacher and ensure that the images are deleted from the device and cloud server immediately after use.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: Print Name: Date:

Appendix C

Emmaus Church of England & Catholic Primary School

Online Safety Policy

Governors have read and understood the relevant Online Safety sections of the DfE document, “**Keeping Children Safe in Education**” (effective 1st September 2023)

Appropriate Filtering

At Emmaus Primary School, we use Liverpool Local Authority as our Internet Service Provider (ISP). This is a safe and secure connection provided by Liverpool City Council/London Grid for Learning which currently uses **WebScreen 3.0** to filter out inappropriate websites.

We recognise that no filtering solution will be perfect but our policy is to ask children (and adults) to let us know if they see something that upsets them or is inappropriate and we will report it to the Local Authority.

Appropriate Monitoring

At Emmaus Primary School, children log on to the computer system using the class identifier in KS1 and KS2, although children use individual identifiers for access to **Purple Mash**.

We have undertaken a risk assessment (1.9.23) looking at the way children access the internet in our school and we are satisfied that the ratio of adults to children as well as the vigilance and the situational awareness of staff would make it very difficult for children to deliberately access inappropriate material.

The governing body will keep Monitoring under review and will look to utilise a technical monitoring situation should the need arise.

As per filtering, we would always encourage children to alert an adult if they see something that upsets them or if they feel it is inappropriate.

Based on the above risk assessment, we have also decided to configure **Swiggle** to be our default search engine for children to use.

Risk Assessment undertaken by:

Mr A. Williams - Headteacher

Mrs C. Yates - Deputy Headteacher & Governor

Appendix D

Online Safety

Acceptable Use Policy (AUP) for PARENTS/CARERS

What is an AUP?

We ask all children, young people and adults involved in the life of Emmaus Primary School to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUP?

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

Where can I find out more?

You can read the school’s full Online Safety Policy on our school website (www.emmausschool.co.uk) for more detail on our approach to online safety and links to other relevant policies. If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher or Computing Lead.

What am I agreeing to?

1. I understand that Emmaus Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting. I agree that the school is not liable for any damages arising from use of internet facilities.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my 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.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school’s online safety policy and not encourage my child to join any platform where they are below the minimum age.
6. I will not share images of other people’s children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous.
7. I understand that the school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the digital images/video permission form and images will never be accompanied by my child’s names.
8. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.
9. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
10. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, maintaining a balance for their social, physical, emotional and mental health.
11. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
12. I can find out more about online safety at Emmaus Primary School by reading the full Online Safety Policy at www.emmausschool.co.uk and can talk to the Headteacher or Computing lead if I have any concerns about my child/ren’s use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~

**I have read, understood and agreed to this policy.**

Signature: \_\_\_\_\_

Name of parent / guardian: \_\_\_\_\_

Parent / guardian of: \_\_\_\_\_

Date: \_\_\_\_\_