St Mary's CE Nursery and Primary School

Felsham Road

Putney

Online Safety Policy

Vision: *Delivering excellence, allowing all to flourish*
Mission: *Creating a culture of wonder, guided by Christian faith*
Values: *Compassion, Endurance, Thankfulness*

April 2026

1. Introduction

1.1. This policy named 'Online Safety Policy' updates and replaces the school's previous policy on e-Safety. Although the terms *e-Safety*, *Internet Safety* and *Online Safety* all mean the same thing, the school will now use the term Online Safety as it better represents the topic it refers to.

1.2. St. Mary's Church of England Primary School is committed to safeguarding its pupils and as online safety is an integral part of safeguarding it therefore requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other documents, such as our Safeguarding and Child Protection Policy, Anti-Bullying Policy and Practice, and our Behaviour Policy and Practice. It complements existing and forthcoming subjects including Health, Relationships and Sex Education and Computing. Any issues and concerns with online safety must always follow our school's safeguarding and child protection procedures.

1.3. Online safety refers to the act of staying safe online. It encompasses the safe and responsible use of technologies and electronic communications that access the internet via computers, laptops, televisions, games consoles, mobile phones, smartphones, tablets and other hand held devices, as well as collaboration tools and personal publishing. It highlights the need to educate children and young people about the benefits and risks of using this technology, emerging technologies and it provides safeguards and awareness for users to enable young people to control their online experience.

1.4. As a Church of England school, we are always guided by our Christian values in supporting the learning of all our children. Compassionate attitudes, concern for the whole person and wider community, trust and respect for one another are just some of the Christian values that are relevant when thinking about issues relating to online safety.

2. Aims

2.1. This policy aims to:

2.1.1. Set out expectations for all St. Mary's CE Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

2.1.2. Help 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, and regardless of device or platform

2.1.3. Facilitate the safe, responsible and respectful 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. This includes the use of AI for both staff and pupils (appendix E).

2.1.4. Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

2.1.4.1. for the protection and benefit of the children and young people in their care

2.1.4.2. for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice

2.1.4.3. for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school andtheir profession

2.1.5. Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns

3. Protecting our school community

3.1. Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardise their security and personal information, lead to unsafe communications or even effect their mental health and wellbeing.

3.2. The main areas of risk for our school community can be summarised as 'The 4 Cs':

3.2.1. Content

3.2.1.1. exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse; misogynistic views

3.2.1.2. lifestyle websites, for example pro-anorexia/self-harm/suicide sites;

3.2.1.3. hate sites;

3.2.1.4. content validation:

3.2.1.5. how to check authenticity and accuracy of online content, increasingly with the use of AI generated images

3.2.1.6. identifying 'fake news' and conspiracy theories

3.2.1.7. spotting disinformation

3.2.2. Contact

3.2.2.1. grooming (sexual exploitation, radicalisation etc.);

3.2.2.2. online/cyber-bullying in all forms;

3.2.2.3. social or commercial identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords;

3.2.3. Conduct

3.2.3.1. aggressive behaviours (bullying) through any digital medium;

3.2.3.2. privacy issues, including disclosure of personal information;

3.2.3.3. digital footprint and online reputation;

3.2.3.4. health and well-being (amount of time spent online (internet or gaming), gambling, body image);

3.2.3.5. sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);

3.2.3.6. copyright (little care or consideration for intellectual property and ownership – such as music and film);

3.2.4. Commerce

3.2.4.1. Access to advertising online that is inappropriate for young people

3.2.4.2. Being tricked into making purchases online

3.2.4.3. Sharing of personal information through online scams or contests

4. End-to-end online safety

4.1. Online safety depends on effective practice at a number of levels:

4.1.1. Responsible computing use by all staff and children (including governors, volunteers, parents/carers, visitors); encouraged by education and made explicit through published policies;

4.1.2. Sound implementation of Online Safety policy in both administration and curriculum, including secure network design and use;

4.1.3. Safe and secure broadband from London Grid for Learning (LGfL) including the effective management of Net Sweeper filtering;

4.1.4. National Education Network (NEN) standards and specifications;

5. Roles and responsibilities

5.1. KCSIE (2025) makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)".

5.2. Filtering and monitoring of online content within the school are the responsibility of the DSL. This is supported by members of the safeguarding team and senior leadership team.

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

5.4. It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

6. Teaching and learning

6.1. In our school's curriculum, the following subjects have the clearest online safety links:

6.1.1. Computing

6.1.2. Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)

6.2. Theme days such as Online Safety Day and STEM day are also opportunities to weave additional digital and online safety into our curriculum at St Mary's

6.3. However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leaders, and making the most of unexpected learning opportunities as they arise. Whenever overseeing the use of technology (devices, the internet, new technology such as AI like ChatGPT, , etc.) in school or setting as home learning tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites. An approved list of uses for AI is included in Appendix E.

6.4. Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular, extended school activities if relevant and remote education), supporting them with search skills, critical thinking (e.g. fake news), 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.

7. Why internet use is important

7.1. At St. Mary's Church of England Nursery and Primary School we believe the internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for both children and staff.

8. Internet use will enhance learning

8.1. At St. Mary's internet access will be designed expressly for children's use and will include filtering appropriate to the age of the children (filtering systems are provided by LGfL). Children will be taught what internet use is acceptable and what is not (a range of e-Safety material and resources are used to support this, such as those set up by the Child Exploitation and Online Protection Centre (CEOP), Children will be given clear objectives for internet use. Children will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.

8.2. We recognise that online safety and broader digital resilience must thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). This framework covers eight areas of online education: self-image and identity; online relationships; online reputation; online bullying; managing online information; health, wellbeing and lifestyle; privacy and security; and copyright and ownership.

9. Children will be taught how to evaluate internet content

9.1. The school will ensure that the use of internet derived materials by both staff and children complies with copyright law. When copying material from the internet it is important for both staff and children to understand issues around plagiarism and to ensure any copyright / intellectual property rights are respected and acknowledged. Children will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy. Part of this education will include the need to be aware that the author of a website / page may have a particular bias or purpose.

10. Introducing the Online Safety Policy to children

10.1. St. Mary's Church of England Primary School implements an Online Safety education programme as part of the computing curriculum and many aspects of online safety also feature in the PSHE/RSHE curriculum. Children across the school are first introduced to the 'BE SMART ONLINE' safety rules:

- **S – Safe:**

  We keep safe by being careful not to give out personal information to people online

- **M – Meeting:**

  We never agree to meet someone we have only met online

- **A – Accepting:**

  We think before we open files, pictures or attachments from people we don't know – they might contain a virus or nasty message

- **R – Reliable:**

  We remember that what we see online may not be true or accurate and that someone online might be lying about who they are

- **T – Tell:**

  We will tell an adult we trust if someone or something makes us feel uncomfortable or worried, including if we are being bullied online

- **♥ – Be Smart with a Heart:**

  We try our best to be kind and respectful to others online

10.2. A poster showing these BE SMART ONLINE safety rules are displayed in all curriculum networked rooms and preferably near to the computers the children have access to (see Appendix A). In the Computing Room, a large display board is dedicated to the BE SMART ONLINE safety rules. The BE SMART ONLINE safety rules are discussed with children throughout the year and form the foundation of our children's understanding of acceptable behaviour when using an online environment. At St. Mary's the younger children will be introduced to Smartie the Penguin. These are a set of stories where 'Smartie' is faced with various digital situations that could be faced when online.

10.3. Children will learn how to use computers safely and how to keep personal information private. As the children progress through the

school the online safety education programme will cover a range of skills and behaviours appropriate to their age and experience, including:

10.3.1. to know their responsibilities through the Acceptable Use Policy – Pupil Agreement (see Appendix B) [This is signed by pupils at the start of the year].

10.3.2. to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;

10.3.3. to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;

10.3.4. to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;

10.3.5. to understand why they must not post pictures or videos of others without their permission;

10.3.6. to have strategies for dealing with receipt of inappropriate materials;

10.3.7. (for older pupils) to understand why and how some people will 'groom' young people for sexual reasons, radicalisation etc.;

10.3.8. (for older pupils) to understand the impact of cyber bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;

10.3.9. to know how to evaluate content they come across to assess its reliability to avoid the spread of misinformation

10.3.10. to understand that they should challenge views that are against school values for example misogynist rhetoric

10.3.11. to know how to report any abuse including cyber bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted member of staff, or an organisation such as Childline or the CLICK CEOP button;

10.4. The school will use a variety of resources and materials to compliment and support our online safety education and these will be sourced from trusted organisations like CEOP, Childnet International, UK Safer Internet Centre, and the NSPCC. Each year the school will actively celebrate Safer Internet Day, usually held sometime in early February, which is a day in the school calendar to promote safer and more responsible use of online technology and mobile phones.

11. Online bullying / Cyber bullying

11.1. Online bullying/Cyber bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends and family. It may include prejudice related to gender, sexual orientation, race, culture, ability, disability, age or religion. The school

takes bullying very seriously and has robust procedures for identifying and dealing with it. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type, including issues arising from banter, will not be tolerated by the school and will be dealt with under the procedures within the Anti-Bullying Policy and Practice and the Behaviour Policy and Practice documents.

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

12. Upskirting

12.1. It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence, as highlighted in Keeping Children Safe in Education (2025) and that pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

13. Sexting

13.1. All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

13.2. Materials to support teaching about sexting can be found at sexting.lgfl.net

14. Sexual violence and harassment

14.1. Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; the case studies section provides a helpful overview of some of the issues which may arise.

14.2. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed

to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

14.3. In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

15. Managing internet access, system security (virus protection), filtering, monitoring, user access and backup

15.1. Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

15.2. Since KCSIE 2025, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring

15.3. Schools are also required to follow the new DfE filtering and monitoring standards, which require them to:

15.3.1. identify and assign roles and responsibilities to manage filtering and monitoring systems

15.3.2. review filtering and monitoring provision at least annually

15.3.3. block harmful and inappropriate content without unreasonably impacting teaching and learning

15.3.4. have effective monitoring strategies in place that meet their safeguarding needs

15.3.5.

15.4. As schools get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams. The safeguarding team will also undertake their own filtering checks on devices within the school, creating an audit trail of devices and login profiles. This duty is taken by one of the school safeguarding team – usually the online safety lead.

15.5. ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over-blocking.

15.6. Our designated computing support member of staff will monitor and review computing systems capacity and security regularly. Virus protection will be updated regularly and security strategies will be discussed with Wandsworth Children's Services computing support. The following is a list of systems in place at St. Mary's to ensure the school's internet access is appropriately managed.

15.7. This school:

15.7.1. Has the educational filtered secure broadband connectivity through the LGfL and therefore connects to the 'private' National Education Network (NEN);

15.7.2. Uses the LGfL Net Sweeper filtering system (Webscreen 3) which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to

the filtering policy is logged and only available to staff with the approved 'web filtering management' status;

15.7.3. Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

15.7.4. Ensures network health through the use of Sophos anti-virus software (provided from LGfL) and network set-up so staff and pupils cannot download executable files;

15.7.5. Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

15.7.6. Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

15.7.7. Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;

15.7.8. Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;

15.7.9. Uses security time-outs on Internet access where practicable / useful;

15.7.10. Uses individual accounts and log-ins for staff and year group accounts as log-ins for pupils;Uses guest accounts for visitors with limited access;

15.7.11. Requires all users to log-off when they have finished working on the computer or are leaving the computer unattended;

15.7.12. Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;

15.7.13. Has regular back-up of school data (curriculum and admin);

15.7.14. Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas such as the Computing Room where older pupils have more flexible access;

15.7.15. Ensures all staff, governors, volunteers and pupils have signed an acceptable use agreement form and understands that they must report any concerns;

15.7.16. Ensures pupils only publish within an appropriately secure environment, for example, the school's learning environment, LGfL secure platforms such as J2Bloggy, etc.

15.7.17. Requires staff to preview websites before use (where not previously viewed or cached) and encourages the use of the school's Learning Platform or Website as a key way to direct students to age / subject appropriate websites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google Safe Search, etc.

15.7.18. Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;

15.7.19. Informs all users that Internet and e-mail use is monitored;

15.7.20. Informs pupils and staff that they must report any failure of the filtering systems directly to their teacher for pupils, or e-Safety coordinator and system administrator for staff. Our system administrator logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary;

15.7.21. Makes clear that staff are responsible for ensuring that any computer, laptop or other equipment loaned to them by the school is used to support their professional responsibilities;

15.7.22. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

15.7.23. Provides advice and information on reporting offensive materials, abuse/ bullying etc. for pupils, staff and parents;

15.7.24. Immediately refers any safeguarding or child protection issues to the Designated Safeguarding Lead;

15.7.25. Immediately refers any material we suspect is illegal to the appropriate authorities – Police/CEOP – and the LA.

15.7.26. Undertakes filtering checks on devices within the school, creating an audit trail of devices and login profiles. These are currently undertaken half termly by the Online Safety Lead.

15.7.27. Undertakes an annual filtering and monitoring healthcheck, provided by LGfL, to address any areas for attention. These are brought to the attention of the technical team for support in resolving when needed.

15.7.28. Utilises the SENSO portal to monitor key strokes from pupils which may pose safeguarding concerns. The DSL has access to this platform and is notified of any 'screengrabs' that have been flagged by the SENSO portal.

16. Authorising internet access

16.1. In line with our belief that the school has a duty to provide children with quality internet access and that internet use is part of the statutory curriculum we at St. Mary's Church of England Primary School assume our parents authorise internet access for their child. If a parent wishes to discuss their child's access to the internet at school they should arrange to speak with the head teacher.

17. Acceptable Use Policy (AUP)

17.1. We ask everyone involved in the life of St. Mary's Church of England Primary School to sign an Acceptable Use Policy (AUP), which 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).

17.2. All children in both Key Stage 1 and Key Stage 2 are required to sign the 'Acceptable Use Policy – Pupil Agreement' class form (see Appendix B). This confirms they have read and understood the online safety rules, and that they will use the school computers, school network and systems, software, hardware, hand-held devices, and the internet in a responsible way, including the use of e-mail and other

forms of communication. These class forms will be signed each year and displayed as a visual reminder. Children are made aware that both computer and Internet use (including e-mail) will be monitored to ensure their safety and that any inappropriate use will be dealt with.

17.3. Equally, all staff members, including governors and volunteers, must sign the 'Acceptable Use Policy – Staff Agreement' form (see Appendix C) to say they have read and understood the online safety rules, and that they too will use the school computers, school network and systems, software, hardware, hand-held devices, and the internet in a responsible way, including the use of e-mail and other forms of communication. The school will keep a record of all staff, governors and volunteers that have completed these forms and the school business manager will ensure that this record is kept up to date – making sure that whenever changes are made a new AUP has been shared and signed. Staff are made aware that both computer and internet use (including e-mail) will be monitored and that any inappropriate use will be dealt with.

17.4. Along with this policy, the AUP will also be reviewed annually. All staff, governors and volunteers have particular legal/professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in this document.

17.5. If you have any questions about the AUP or our approach to online safety, please speak to our online safety coordinators, designated safeguarding lead or senior leadership team.

18. Misuse of internet access and school technology

18.1. We have clear and well communicated rules and procedures 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 (AUP) as well as in the relevant sections of this document. Where pupils contravene these rules, the school's behaviour policy and practice will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

18.2. It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning or remote education that may take place in future periods of closure/quarantine etc. 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.

19. Managing unsuitable content

19.1. The school will work with the LA, DfE, CEOP, UK Safer Internet Centre and the Internet Service Provider to ensure systems to protect children are reviewed and improved. This is organised mainly by the LGfL but checks are made by the online safety lead, along with any designated computing support staff members of staff. The DSL will ensure that regular checks are made to make sure that the filtering

methods selected are appropriate, effective and reasonable. Filtering checks are conducted half termly by the online safety lead or member of the safeguarding team.

19.2. If staff or children do discover an unsuitable site, including coming across inappropriate or illegal content, it must be reported to the online safety coordinator immediately. Any safeguarding or child protection issues must be reported immediately to the Designated Safeguarding Lead.

20. Safety Button

20.1. At St. Mary's any computer connected to the curriculum server should have a 'Safety Button' installed:The Big Red Button. The Big Red Button usually found in the top right corner of the computer screen. The children are taught that if something on-screen upsets or worries them, perhaps they might feel uncomfortable by what they have seen or heard, they should immediately click on Hector or the Big Red Button. Once activated, the computer screen will be covered (a mushroom explosion scene for the Big Red Button) and a written message appears to instruct the child to get adult help.

20.2. When a child the Big Red Button all staff should follow this protocol:

20.2.1. Check with the child they have clicked the button for a genuine reason and that it was not clicked by accident;

20.2.2. Explain they have done the right thing and that the content that upset or concerned them can no longer be seen or heard;

20.2.3. If the child appears upset or distressed support them as necessary;

20.2.4. Protecting the child and others around them, ensure no one can see the computer screen and view the content yourself to make a judgement of whether it is inappropriate or unsuitable;

20.2.5. If the content if found to be inappropriate or unsuitable take a copy of the URL (web address) and print this to a printer for collection;

20.2.6. Immediately collect the printed URL and if necessary add any relevant details such as date and time, search terms typed, website used etc. Remember to keep the screen covered if away from the computer or navigate away from the offending content;

20.2.7. As a matter of urgency pass on the printed URL and relevant details to either the online safety coordinator or designated safeguarding lead who will then contact LGfL to filter or block the content, the DSL may also be able to block content locally (if the content is illegal or particularly disturbing the police may also be contacted);

20.2.8. If the content is not deemed to be inappropriate or offensive there is no need to pass on the details. However, if the content is of a sensitive nature that has caused the child to click on the Big Red Button it may be appropriate for staff to have a discussion with the child and determine ways to avoid coming across content they find sensitive, for example, teaching them to

use 'safe' keywords in a search or perhaps avoiding the use of an image search;

21. Disclaimer and assessing risks

21.1. St. Mary's School will take all reasonable precautions to ensure that children access only appropriate material. However, due to the international scale and linked nature of internet content, which is also rapidly evolving, it is not possible to guarantee that unsuitable material will never appear on a computer or hand-held device for which the school is responsible. Neither the school, Diocese of Southwark or Wandsworth Borough Council can accept liability for the material accessed, or any consequences of internet access. The school will audit our computing and internet provision annually to establish if the online safety policy is adequate and that its implementation is effective.

22. Electronic Mail (e-mail)

22.1. At St. Mary's staff, including governors, are provided with an e-mail account for their professional use and for conducting all school business (this service is provided by LGfL). Staff know that e-mail sent to an external organisation must be written carefully, and may require authorisation, in the same way as a letter written on the school headed paper. Staff are also made clear that personal e-mail should be conducted through a separate account. Staff can communicate with our parent body through a dedicated class LGfL e-mail account (known at St. Mary's as PACT e-mail). Staff are reminded to use 'blind carbon copy' (Bcc) when e-mailing more than one parent contact.

22.2. Our children, from Year 3 upwards (once they have been introduced to e-mail), may only use approved e-mail accounts on the school system. They will have access to this account whilst at the school and the account will be deleted when they leave. The children are taught about the safety and 'netiquette' of using e-mail both in school and at home. They must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Children must immediately tell a member of staff if they receive an offensive e-mail and details of this should be passed on to the online safety coordinator who may contact the police. Children are taught not to respond to any malicious or threatening e-mail, nor to delete them, but to keep them as evidence of bullying. Both staff and children are aware that the forwarding of 'chain' e-mail letters is not permitted. Embedding adverts is also forbidden.

22.3. Staff, governors and pupils are made aware that e-mail accounts are monitored.

23. Published content and the school website

23.1. St. Mary's maintains a school website with the following web address: http://www.stmarysschoolputney.co.uk

23.2. The contact details on our school website are the school's address, e-mail and telephone number. A wealth of information is available to view on the school website. Staff and children's personal information will not be published. Both the computing subject leader

and designated computing support member of staff will be responsible for maintaining and updating the school's website. The head teacher, with the support of the governing body, will take overall responsibility to ensure that content is accurate, appropriate and the quality of presentation is maintained. They will also ensure the school website complies with statutory DfE requirements. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity. Any photographs of the children published on the web do not have full names attached. Likewise, the school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website. Since January 2017 the school has also maintained a Twitter and Facebook account (see below) with a 'timeline' feed embedded on the school website.

24. Publishing children's images and work

24.1. Photographs and videos that include children will be selected carefully and will not identify children by their full name. Children's full names will not be used anywhere on the website. Written permission from parents or carers will be obtained before photographs and videos of children are published. Permission is also required from staff if photographs and videos of staff are published. Children's work can only be published with the permission of the child and parents.

25. Social networking and personal publishin

25.1. St. Mary's Church of England Primary School will either block or filter access to social networking sites, but may allow them for specific supervised activities, including staff access to the school's own social network sites (not currently in place and are under review). Staff are instructed to always keep professional and private communication separate. Staff are instructed not to run social network spaces for children or to open up their own personal spaces to their students. Staff should not be online friends with any pupil. Any exceptions must be approved by the head teacher. Staff are also reminded for their own welfare to avoid engaging in any online discussion on personal matters relating to members of the school community and that any personal opinions posted online should not be attributed to either the school, the Diocese of Southwark or Wandsworth Borough Council. Personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute. Newsgroups will be blocked unless specific use is approved by the head teacher.

25.2. Children will be advised never to give out personal details of any kind which may identify them, others or their location. Children are reminded to not share e-mail addresses without permission and to use 'blind carbon copy' (Bcc) when e-mailing more than one contact. They will be taught about social networking, acceptable behaviours and how to report any misuse, intimidation or abuse. St. Mary's has previously usedits own official Twitter and Facebook accounts, @PutneySMPS, and uses these in a professional context as a form of communication to parents and the wider community. The purpose of the school's Twitter and Facebook accounts are to act as blogs to document school

activity in near real time. The use of social media of the school is under review.

26. Cloud environments, storage and digital learning platforms

26.1. At St. Mary's the use of cloud storage technology, cloud learning environments and digital learning platforms are something that has emerged recently through school closures and lockdowns at the time of the coronavirus pandemic. The school has utilised cloud environments and digital platforms through its delivery of remote education during the pandemic. The school has made use of services provided by Microsoft Office 365 for Education and is using the Microsoft Teams digital learning platform for delivering remote education. This system is still in place should the need arise again. It may also be used in the future to move our network files to 'the cloud'.

26.2. In developing our use of cloud environments, the school will ensure it adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. The uploading of any information and files to a cloud environment by staff members is only done according to their professional responsibilities. Presently only LGfL cloud storage and partner platforms (e.g. myDrive, G Suite, Microsoft 365) are approved for use by the school. Photographs and videos uploaded should only be accessible by members of the school community. Any media made public is done so with parental permission.

27. Managing video-conferencing and video-telephony

27.1. Video-conferencing and video-telephony enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. At school IP video-conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet. Children should ask permission from the supervising member of staff before making or answering a video-conference call. Use of webcams will only ever be used for specific learning purposes and video-conferencing is always fully supervised by a member of the teaching staff in a secure environment. The use of this for pupils is extremely rare.

27.2. There are an increasing number of video-telephony services and applications available that emulate traditional video conferencing (e.g. Skype, Zoom, Microsoft Teams) via computers, tablets, mobile phones, consoles etc. and many of these services incorporate additional features such as instant messaging and chat, application integration, recording, file and desktop sharing. The relative ease, lack of equipment needed and portable nature of these services and applications means that in recent times they are being used to provide distance/remote learning (learning away from the school setting) at times of school closure or when pupils and staff are unable to attend school. At St. Mary's these services and applications will be used as the school deems necessary, for example, participating in virtual

meetings for staff and governors when these members are away from the school setting and for delivering remote education when pupils are unable to attend. When video-telephony is used the people involved must adhere to the guidelines for safe and secure use for the service/application being used. In the event of a school closure, the school can use Microsoft Teams to deliver remote education to pupils, and including 'livestreaming' lessons. Our staff will ensure they follow the 'Twenty Safeguarding Considerations for Lesson Livestreaming' – suitable for all types of online learning (see Appendix D).

27.3. See the school's separate Remote Education policy for further details.

28. Managing emerging technologies

28.1. At St. Mary's we will always examine emerging technologies for educational benefit and the computing subject leader will carry out a risk assessment before use is allowed by children and staff.

29. Protecting personal data and data security

29.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation, or GDPR). All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls,filtering and monitoring all support data protection.

29.2. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

29.3. The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information. Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. GDPR training is undertaken regularly. The use of USO-FX and Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

29.4. GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net

30. Mobile phones, smart watches and other personal hand held devices

30.1. Mobile phones, smart watches and other personal hand-held devices brought into school are entirely at the owner's own risk. The school accepts no responsibility for the loss, theft or damage of any mobile phone, smart watch or hand-held device brought into school.

30.2. All staff should keep mobile phones in a secure place during working hours and they should not be used during contact time with

the children. All visitors are requested to keep their mobile phones on silent. Smart watches worn should also be kept on silent mode and are not be used to communicate during contact time. The recording, taking and sharing of images, video and audio on any mobile phone, smart watch or personal hand-held device is to be avoided; except where it has been explicitly agreed otherwise by the head teacher.

30.3. The school reserves the right to search the content of any mobile phone, smart watch or hand-held device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring. Children are not permitted to have mobile phones upon their person in school. We recognise that our Year 5 and Year 6 pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. These pupils must hand in their mobile phone to the school office immediately on arrival where they will be stored for the duration of the day and collected at the end of the day. Children wearing smart watches must disable syncing to mobiles.

30.4. We would ask all parents to consider:

30.4.1. Is your child's mobile phone registered for a child's use with the provider?

30.4.2. Do you know how your child's phone works?

30.4.3. Have you agreed passwords with your child/ren and do you check the content of texts and any activity on social networking sites?

30.4.4. Can you turn off the Internet access on your child's phone?

30.4.5. Can you install a child safe Internet version on your child's phone?

30.4.6. Do you know what your child is viewing and participating in, on the Internet?

30.4.7. Is your child emotionally mature enough to use a mobile phone/the Internet independently?

31. Searching, screening and confiscation

31.1. Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

31.1.1. cause harm

31.1.2. disrupt teaching

31.1.3. break school rules

31.1.4. commit an offence

31.1.5. cause personal injury

31.1.6. damage property

31.2. Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

31.3. Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.

32. Parental Support with online safety

32.1. The online safety policy will be made available to all stakeholders via the school website. Parents and carers are asked to read, understand and promote the school's Acceptable Use Policy – Pupil Agreement (see Appendix B) with their children.

32.2. St. Mary's gains parental/carer permission for use of digital photography or video involving their child as part of the school agreement form completed when their child joined the school. Parents are allowed to take photographs and videos of their children (for personal use only) at school events. Parents are reminded that they should not take photographs or video of other children or members of staff unless permission has been sought. Parents are also reminded to avoid uploading/posting photography or video onto any social media or social networking site.

32.3. St. Mary's expects parents to support the school in promoting online safety through its aim of offering a rolling programme of online safety advice, guidance and training (dependent on interest and funding).

33. Using the internet safely at home – guidance for parents

33.1. Many Internet Service Providers offer filtering systems and tools to help safeguard children at home, however, it remains surprisingly easy for children to access inappropriate material. Parents are advised to set the security levels within their internet browsers with this in mind. It is worth considering locating the computer in a family area where possible (not a bedroom). It might also be possible to limit the availability of your internet connection to certain times during the day. These measures will help enable supervision of internet use. Whilst not denying children opportunities to learn from and enjoy the incredibly wide range of material and games on offer on the internet, it is important to consider what access children have to the internet on their mobile phones, games consoles and other devices and discuss with them some simple strategies and rules to enable them to stay safe. Parents are encouraged to call their Internet Service Providers to find out more on the parental controls available.

33.2. Support for parents and carers to keep their children safe online includes:

33.2.1. Internet matters - for support for parents and carers to keep their children safe online

33.2.2. London Grid for Learning - for support for parents and carers to keep their children safe online

33.2.3. Thinkuknow - for advice from the National Crime Agency to stay safe online (CEOP)

33.2.4. UK Safer Internet Centre - advice for parents and carers

33.2.5.

33.3. Guidelines suggest that children should:

33.3.1. Ask permission before using the internet and discuss what websites they are using;

33.3.2. Only use websites agreed with parents;

33.3.3. Agree on a time period or time limit to access the internet

33.3.4. Only e-mail people they know;

33.3.5. Ask permission before opening an e-mail sent by someone they don't know;
33.3.6. Not use their real name when using games or website on the Internet (create a nickname);
33.3.7. Never give out personal information about themselves, friends or family online;
33.3.8. Never arrange to meet someone they have 'met' on the internet;
33.3.9. Not create accounts with social media sites if under the age limit.

34. Handling online safeguarding concerns and incidents

34.1. It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship). General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side caution by talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

34.2. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

34.3. School procedures for dealing with online safety will be mostly detailed in the following policies:
34.3.1. Safeguarding and Child Protection Policy
34.3.2. Anti-Bullying Policy
34.3.3. Behaviour Policy
34.3.4. Acceptable Use Policies
34.3.5. UK GDPR Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

34.4. This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

34.5. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

34.6. Any concern/allegation about staff misuse is always 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 the LADO (Local Authority's Designated Officer).

35. Further help and support

35.1. Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding and Child Protection Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations we work with may also have advisors to offer general support.

35.2. Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff and govenors, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

36. Writing and reviewing the online safety policy

36.1. St. Mary's online safety policy will operate in conjunction with other policies:

36.1.1. Safeguarding and Child Protection Policy
36.1.2. Behaviour Policy and Practice
36.1.3. Anti-Bullying Policy and Practice
36.1.4. Computing Policy
36.1.5. PSHE Policy (and RSHE Policy)
36.1.6. UK GDPR Data Protection Policy
36.1.7. Social Media Policy
36.1.8. Remote Education Policy

37. 2025-26 arrangements

37.1. Designated Safeguarding Lead

Cheryl Payne – Headteacher

37.2 Deputy Designated Safeguarding Lead

Gemma Jennings – Deputy Head Teacher
Kerry Dunford – Inclusion Manager
James Phillips – Senior Teacher

37.3 Online Safety Coordinators

James Phillips - Computing Subject Leader
Monica Read - Computing Support

37.4 Our Online Safety Policy and Acceptable Use Policy has been written by the school, building on previous e-Safety policies, LGfL's safeguarding resources and model online safety and acceptable use policies, as well as government guidance. It has been agreed by all staff and approved by governors.

The Online Safety Policy, Acceptable Use Policy (AUP) and its implementation will be reviewed annually. Following this review the policy will be made available to all stakeholders via the school website.

Name/s and job title of reviewer	Date of review	Date of governor approval	Suggested date for review
Mr Mark Lett	July 2024	July 2024	September 2025
Mr James Phillips	April 2026		April 2026

APPENDIX A

BE SMART ONLINE SAFETY RULES

APPENDIX B

Acceptable Use Policy – Pupil Agreement

St Mary's CE Primary School
Acceptable Use Policy
Pupil Agreement

All pupils should recognise that the safe and responsible use of computer facilities in this school, including internet access, is as an essential part of their learning, as required by the National Curriculum. Pupils are asked to sign this class form to show that both the statements and online safety rules have been understood and agreed.

Class: Year X Date: 2025-2026

Pupil's Agreement

- I have read and I will follow the BE SMART ONLINE safety rules.
- I only use computers, devices, apps, sites and games when I am allowed to and have permission (whether at home or at school).
- I don't behave differently online or when I'm learning at home, so I don't say or do things I wouldn't do in the classroom.
- I will use the computers, school network and systems, digital learning platforms, software, hardware, hand held devices and other new technologies in a safe and responsible way at all times.
- I will use the internet, including the use of e-mail and other forms of communication, in a safe and responsible way at all times.
- I will tell a trusted adult if I am upset, worried, scared or confused, including if I get a funny feeling in my tummy about something.
- I don't change clothes or get undressed in front of a camera.
- I know that the school network, devices, digital learning platforms and internet access may be monitored.

Signed:

St Mary's CE Primary School
Acceptable Use Policy
Staff Agreement

For all staff, governors and volunteers

This staff agreement form covers the use of computers, school network and systems, intranet, internet, social media, digital learning platforms and cloud storage environments, e-mail, software, hardware, equipment, hand held devices and other new digital and electronic technologies.

- I have read and understood St. Mary's Church of England Primary School's full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.

- I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.

- I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) and make them aware of new trends and patterns that I might identify.

- I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).

- I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.

- I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!

- I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

- I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum,

supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

- I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL.

- I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

- During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.

- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

- I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas as outlined in KCSIE, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

- I understand the details on social media behaviour, the general capture of digital images/video and on my use of personal devices as stated in the full Online Safety Policy. If I am ever not sure, I will ask first.

- I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

- I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

- I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

- I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

- I will not reveal my password(s) to anyone. I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access work e-mail / internet / intranet / network, digital learning platforms or other school / LA systems.

- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.

- I will only use the approved, secure e-mail system(s) for any school business. This is currently: LGfL StaffMail (powered by Outlook)

- I will only use the approved school e-mail; school digital learning platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.

- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other 'defence' systems.

- I will not use personal digital cameras or camera phones or digital devices for taking and transferring images of pupils or staff without permission

from the headteacher and will not store images at home without permission.

- I will follow the school's policy on the use of mobile phones / devices at school and will not use them during contact time with children.
- I will use the school's digital learning platform in accordance with school protocols – as defined in the Remote Education Policy, incorporating Microsoft Teams User Agreement and Code of Conduct.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or hand held device loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching (for staff with teaching responsibilities).
- I will only use LA systems in accordance with any corporate policies.
- I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.

User Signature

Full Name: _____ (printed)

Job title: _____

I agree to abide by all the points above.

I understand that it is my responsibility to remain up-to-date with online safety requirements and to read and understand the school's most recent online safety and safeguarding polices.

I wish to have an e-mail account; be connected to the intranet & internet; be able to use the school's digital learning platform, computing resources and systems.

I understand that the school network, computing systems, devices and internet access, including the use of e-mail and digital learning platform, may be monitored.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____ Date: _____

Authorised Signature

Full Name: _____ (printed)

Job title: _____

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____ Date: _____

APPENDIX D

Twenty Safeguarding Considerations for Lesson Livestreaming
(and all online learning)

Twenty Safeguarding Considerations for Lesson Livestreaming

Just because schools are supporting students remotely and sending work home does NOT mean that you need to livestream lessons.
This should only be done where you are equipped to do so safely. But if you are considering it, bear these things in mind:

1. Only use school-registered accounts, never personal ones
2. Don't use a system that your SLT has not approved
3. Will some students be excluded? Do they have internet, a device and a quiet place?
4. Do students and staff have a safe and appropriate place with no bedrooms or inappropriate objects/information visible?
5. Check the link in an incognito tab to make sure it isn't public for the whole world!
6. Has your admin audited the settings first (who can chat? who can start a stream? who can join?)
7. What about vulnerable students with SEND and CP needs?
8. Don't turn on streaming for students by mistake – joining a stream ≠ starting a stream
9. Never start without another member of staff in the 'room' and without other colleagues aware
10. Once per week may be enough to start with – don't overdo it and make mistakes.
11. Keep a log of everything - what, when, with whom and anything that went wrong
12. Do you want chat turned on for pupils? Can they chat when you aren't there?
13. Avoid one-to-ones unless pre-approved by SLT
14. Remind pupils and staff about the AUP agreements they signed* The rules are the same
15. Remind pupils and staff about the safeguarding policy and reporting process – does it work remotely?
16. Do you want to record it? Are students secretly recording it? You may not be able to tell.
17. How can students ask questions or get help?
18. What are the ground rules? When can students speak / how?
19. If you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.
20. Is your DPO happy? GDPR covered? Parental consent needed?

THE DIGISAFE TEAM WILL BE EXPLORING SAFE SETTINGS FOR THE MAIN PLATFORMS
CHECK OUR SOCIAL PAGES
@LGfLDigiSafe

* Need templates?
See safepolicies.lgfl.net

LGfL DigiSafe
keeping children safe

Appendix E – **Approved Uses of AI and Rationale**

Below is a practical **approved activities list** for teachers using AI at St Mary's. It aligns with current guidance from the UK **Department for Education (DfE)**, the **Information Commissioner's Office (ICO)**, and wider best practice (NCSC/UNESCO).

Why Copilot (our chosen AI assistant)

- **Enterprise protections under our Microsoft agreement**: Copilot operates within Microsoft 365's compliance framework (e.g., GDPR, EU Data Boundary commitments) and **does not train on our tenant data**. Staff must sign in with their school account and save work in Microsoft 365. [learn.microsoft.com]
- **Education sector due-diligence**: Independent assessments and sector briefings (e.g., Jisc updates; DPIAs) note the move to enterprise-level protections for signed-in institutional users and set out considerations schools should apply. [nationalce…nvolve.org], [surf.nl]

Note on our AI platform:
Microsoft Copilot is the school's chosen AI assistant. Staff must use Copilot signed in with their school account, as it benefits from Microsoft's enterprise security, privacy and data protection commitments (including that prompts/responses and Graph data are **not used to train foundation models**) under our EdTech contract. [learn.microsoft.com]

Teacher-facing, low-risk uses

1. **Drafting and improving lesson plans, schemes of work, and curriculum maps**
   Use Copilot to generate outlines, success criteria, differentiation ideas, and vocabulary lists; always review for accuracy and suitability before use. DfE emphasises these workload-reducing, teacher-facing uses as near-term, lower risk. [gov.uk], [educationh…log.gov.uk]
2. **Creating classroom resources**
   Generate slides, worksheets, knowledge organisers, visual aids, word banks, and age-appropriate texts (e.g., at specific reading ages). Teachers *must check factual accuracy and appropriateness*. [schoolsweek.co.uk]
3. **Formative assessment support**
   Create quizzes, exit tickets, and exam-style practice questions from teacher-selected content; draft feedback statements for common misconceptions, with the teacher retaining final responsibility. Avoid using AI for high-stakes, summative judgements. [schoolsweek.co.uk], [post.parliament.uk]
4. **Differentiation and inclusion**
   Suggest scaffolds, sentence starters, alternative representations, and tailored reading passages to support diverse learners and SEND. Teachers supervise and adapt outputs; AI augments, not replaces, pedagogy. [assets.pub…ice.gov.uk]
5. **Drafting parent/carer communications**
   Produce **first drafts** of letters/emails (e.g., trip notices, reminders) that staff then edit and approve. Do not include personal data about individual pupils in prompts. [schoolsweek.co.uk], [gov.uk]

6. **Administrative efficiency**
   Summarise staff meeting notes; draft policy updates, CPD overviews, rota/timetable options, and task lists—always with human review. [schoolsweek.co.uk]
7. **Professional reflection and CPD**
   Generate CPD plans, research summaries, and observation note templates; cross-check with trusted sources and school priorities. [assets.pub…ice.gov.uk]
8. **Resource localisation and language support**
   Draft plain-English versions of documents or provide first-pass translations for school communications; teacher reviews final text for tone and accuracy. [educationh…log.gov.uk]
9. **Creative prompts for writing and projects**
   Generate age-appropriate story starters, character ideas, and project themes. Teachers curate and frame for the class; pupils' engagement stays guided by teacher instruction. [gov.uk]

Carefully supervised pupil-facing uses (when permitted by school policy) – Pupil facing use is not yet permitted

DfE advises **great care** for pupil use; schools must meet legal duties on data protection, safeguarding, IP, and filtering/monitoring. In primary settings, pupil access should be **structured, supervised, and age-appropriate**, with clear learning objectives. [gov.uk]

11. **Critical digital literacy activities**
    Teacher-led exploration of how AI works, evaluating reliability/bias, and distinguishing AI-generated content—using safe, school-approved tools under supervision. [assets.pub…ice.gov.uk], [unesco.org]
12. **Guided idea generation**
    Pupils co-create brainstorming lists or vocabulary with the teacher mediating prompts in a whole-class or small-group format; no personal data is entered. [gov.uk], [gov.uk]
13. **Accessibility supports (teacher mediated)**
    Teacher uses AI to produce alternative explanations or reading passages in class; outputs are displayed or distributed by the teacher rather than pupils querying AI directly. [assets.pub…ice.gov.uk]

Guardrails and conditions of use (apply to all activities)

- **Professional judgement and human oversight**
  Teachers remain responsible for the accuracy, appropriateness, and safety of any AI-generated content. AI should support, not replace, teacher expertise. [educationh…log.gov.uk]

- **No personal/sensitive data in prompts**
  Do **not** enter pupil names, addresses, medical/SEND details, assessment records, or any identifiable information into generative AI prompts. Consult the DPO/IT lead if in doubt. [gov.uk]
- **Intellectual property and copyright**
  Respect intellectual property in inputs and outputs; avoid using copyrighted material without permission; be transparent about AI use where relevant. [gov.uk]
- **Safeguarding and filtering/monitoring**
  At present, generative AI is blocked using our filtering system. **If and when** pupil-accessible AI becomes available it must be behind school filtering/monitoring, with clear rules and staff supervision. It will then be aligned with up to date KCSIE and DfE product safety expectations for generative AI. [assets.pub…ice.gov.uk], [gov.uk]
- **Risk assessment and governance**
  Conduct/record DPIAs for pupil-facing use or where personal data could be processed; clarify controller/processor roles with vendors; ensure contracts and technical controls are in place. [ico.org.uk], [brownejacobson.com]
- **Secure, approved tools only**
  Use enterprise-protected tools (e.g., Copilot with school sign-in) and avoid consumer AI sites for school work. Follow NCSC secure-by-design principles and school IT policies. [ncsc.gov.uk], [learn.microsoft.com]
  '***Schools*** and colleges must not allow or cause students' original work to be used to train generative ***AI*** models unless they have permission' (DfE, 2025)
- **Age appropriateness and inclusion**
  Follow UNESCO's human-centred guidance:prioritise inclusion, equity, and age-appropriate use; validate tools before pupil exposure. [school-edu….europa.eu], [news.un.org]

Quick-reference: Approved activities summary

- ✅ Plan lessons, schemes, and units (teacher-facing). [gov.uk]
- ✅ Create slides/worksheets/knowledge organisers (teacher-facing). [schoolsweek.co.uk]
- ✅ Draft formative quizzes and feedback (teacher review required; avoid high-stakes summative use). [schoolsweek.co.uk], [post.parliament.uk]
- ✅ Differentiate resources and produce accessibility variants (teacher-mediated). [assets.pub…ice.gov.uk]
- ✅ Draft parent/carer letters and general communications (no personal data in prompts). [schoolsweek.co.uk], [gov.uk]
- ✅ Summarise meetings/policies/CPD notes (human oversight). [schoolsweek.co.uk]
- ✅ Support discussion of anonymised data trends (do not prompt with identifiable data). [gov.uk], [post.parliament.uk]
- ✅ Generate creative writing prompts and age-appropriate texts (teacher review). [gov.uk]

Implementation (for SLT/subject leads)

- Update staff **Acceptable Use Policy** and **AI in Teaching** guidance to reflect the above uses and guardrails. [gov.uk]
- Ensure staff access AI **only via Copilot** (school account) and log usage within normal data governance. [learn.microsoft.com]
- Keep a light-touch register of **AI-assisted resources** (what, where used), which aids transparency and review. [assets.pub…ice.gov.uk]
- Provide short CPD on **fact-checking, bias awareness, and age-appropriateness**. [assets.pub…ice.gov.uk]
- If pupil facing use is implemented, a Data Protection Impact Assessment must be conducted (DPIA).

*This list of approved uses and rationale was created with the support of AI. It has then be reviewed before inclusion in this policy.