St Mary's CE 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*

May 2021

Introduction

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.

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' 2020 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 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 follow our school's safeguarding and child protection procedures.

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 and provides safeguards and awareness for users to enable them to control their online experience.

As a Church of England school we are always guided by our Christian values in supporting the learning of all our children. Loving and caring 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.

Aims

This policy aims to:

- 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)
- 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
- 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
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and

    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns

Protecting our school community

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.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content;

Contact

- grooming (sexual exploitation, radicalisation etc.);
- online/cyber bullying in all forms;
- social or commercial identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords;

Conduct

- aggressive behaviours (bullying)
- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (internet or gaming), gambling, body image);
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- copyright (little care or consideration for intellectual property and ownership – such as music and film);

End-to-end online safety

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

- Responsible computing use by all staff and children (including governors, volunteers, parents/carers, visitors); encouraged by education and made explicit through published policies;
- Sound implementation of Online Safety policy in both administration and curriculum, including secure network design and use;
- Safe and secure broadband from London Grid for Learning (LGfL) including the effective management of Net Sweeper filtering;
- National Education Network (NEN) standards and specifications;

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning 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.

Teaching and learning

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

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

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and 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 augmented reality, 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.

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.

Why internet use is important

At St. Mary's Church of England 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.

Internet use will enhance learning

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), which includes Hector's World, Lee and Kim's Adventures and Play Like Share). 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.

We recognise that online safety and broader digital resilience must be 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.

Children will be taught how to evaluate internet content

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.

Introducing the Online Safety Policy to children

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

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 Hector's World – a series of animated episodes and accompanying lessons supported by CEOP. 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:

- to know their responsibilities through the Acceptable Use Policy – Pupil Agreement (see Appendix B)
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- 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;
- to understand why they must not post pictures or videos of others without their permission;
- to have strategies for dealing with receipt of inappropriate materials;
- (for older pupils) to understand why and how some people will 'groom' young people for sexual reasons, radicalisation etc.;
- (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;
- 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;

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.

Online bullying / Cyber bullying

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.

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

Upskirting

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

Sexting

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.

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

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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.

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

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.

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and therefore connects to the 'private' National Education Network (NEN);
- 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;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- 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;
- 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;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- 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;
- Uses security time-outs on Internet access where practicable / useful;
- Uses individual accounts and log-ins for staff and year group accounts and log-ins for pupils;
- Uses guest accounts for visitors with limited access;
- Requires all users to log-off when they have finished working on the computer or are leaving the computer unattended;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Has regular back-up of school data (curriculum and admin);
- 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;
- Ensures all staff, governors, volunteers and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment, for example, the school's learning environment, LGfL secure platforms such as J2Bloggy, etc.
- 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.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet and e-mail use is monitored;
- 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;
- 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;
- 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;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. for pupils, staff and parents;
- Immediately refers any safeguarding or child protection issues to the Designated Lead for Safeguarding;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police/CEOP – and the LA.

Authorising internet access and AUP (Acceptable Use Policy)

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. 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.

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 designated computing support member of staff will ensure that this record is kept up to date. 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.

Misuse of internet access and school technology

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. 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.

Managing unsuitable content

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. The online safety coordinator, along with the designated computing support member of staff, will ensure that regular checks are made to make sure that the filtering methods selected are appropriate, effective and reasonable. 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 Lead for Safeguarding.

Safety Button

At St. Mary's any computer connected to the curriculum server should have a 'Safety Button' installed. This will either be Hector's World Safety Button (an e-Safety tool supported by CEOP) or The Big Red Button. Hector is a dolphin, who is found swimming in the top right corner of the computer screen, and is a character the children will recognise from the associated Hector's World online safety resources. The Big Red Button is also 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 (this will be an underwater scene with accompanying sound effects for Hector or mushroom explosion scene for the Big Red Button) and a written message appears to instruct the child to get adult help.

When a child has activated Hector's World Safety Button or the Big Red Button all staff should follow this protocol:

- Check with the child they have clicked the button for a genuine reason and that it was not clicked by accident;
- Explain they have done the right thing and that the content that upset or concerned them can no longer be seen or heard;
- If the child appears upset or distressed support them as necessary;
- 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;
- 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;
- 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;
- As a matter of urgency pass on the printed URL and relevant details to either the online safety coordinator or designated computing support member of staff who will then contact LGfL to filter or block the content (if the content is illegal or particularly disturbing the police may also be contacted);
- 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 Hector/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;

Disclaimer and assessing risks

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.

Electronic Mail (e-mail)

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.

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.

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

Published content and the school website

St. Mary's maintains a school website with the following web address: http://www.stmarysschoolputney.co.uk
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 account (see below) with a 'timeline' feed embedded on the school website.

Publishing children's images and work

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.

Social networking and personal publishing

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 (presently Facebook and Twitter). 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. 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 been using its 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.

Cloud environments, storage and digital learning platforms

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. 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.

Managing video-conferencing and video-telephony

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.

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. During the coronavirus pandemic, the school used Microsoft Teams to deliver remote education to pupils, and this included some 'livestreaming' lessons. This approach to education will continue to be used for future school closures and our staff will ensure they follow the 'Twenty Safeguarding Considerations for Lesson Livestreaming' – suitable for all types of online learning (see Appendix D).

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

Managing emerging technologies

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.

Protecting personal data and data security

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 and filtering all support data protection.

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.

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. 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.

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

Mobile phones and other personal hand held devices

Mobile phones 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 or hand-held device brought into school. 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. The recording, taking and sharing of images, video and audio on any mobile phone or personal hand held device is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. The school reserves the right to search the content of any mobile phone 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.

We would ask all parents to consider:

- *Is your child's mobile phone registered for a child's use with the provider?*
- *Do you know how your child's phone works?*
- *Have you agreed passwords with your child/ren and do you check the content of texts and any activity on social networking sites?*
- *Can you turn off the Internet access on your child's phone?*
- *Can you install a child safe Internet version on your child's phone?*
- *Do you know what your child is viewing and participating in, on the Internet?*
- *Is your child emotionally mature enough to use a mobile phone/the Internet independently?*

Searching, screening and confiscation

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:

- cause harm
- disrupt teaching
- break school rules
- commit an offence
- cause personal injury
- damage property

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.

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.

Parental Support with online safety

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. 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. 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). The school sends home reading material such as the *Digital Parenting* magazine on an annual basis and parents/carers are encouraged to read this as it is full of useful information about online safety issues and the use of technology.

Using the internet safely at home – guidance for parents

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 Internet Explorer or other 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.

Suggested guidelines for parents for children using the internet

Children should:

- *Ask permission before using the internet and discuss what websites they are using;*
- *Only use websites agreed with parents;*
- *Agree on a time period or time limit to access the internet;*
- *Only e-mail people they know;*
- *Ask permission before opening an e-mail sent by someone they don't know;*
- *Not use their real name when using games or website on the Internet (create a nickname);*
- *Never give out personal information about themselves, friends or family online;*
- *Never arrange to meet someone they have 'met' on the internet;*
- *Not create accounts with social media sites if under the age limit.*

Handling online safety complaints

The online safety coordinator will deal with complaints of internet misuse. Any complaint about staff misuse must be referred to the head teacher. Any complaint about head teacher misuse must be referred to the Chair of Governors. Complaints of a safeguarding or child protection nature must be dealt with in accordance with child protection procedures and reported to the Designated Safeguarding Lead. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Further help and support

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.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, 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.

Addendum during coronavirus pandemic:
Children and online safety away from school

The information in this section has been taken from DfE guidance published on 27th March 2020 (*Coronavirus (COVID-19): safeguarding in schools, colleges and other providers*). All schools and colleges should be doing what they reasonably can to keep all of their children safe. In most cases, the

majority of children will not be physically attending the school or college. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the child protection policy and where appropriate referrals should still be made to children's social care and as required the police.

The department is providing separate guidance on providing education remotely. It will set out 4 key areas that leaders should consider as part of any remote learning strategy. This includes the use of technology. Recently published guidance from the UK Safer Internet Centre on safe remote learning and from the London Grid for Learning on the use of videos and livestreaming could help plan online lessons and/or activities and plan them safely.

All schools and colleges should consider the safety of their children when they are asked to work online. The starting point for online teaching should be that the same principles as set out in the school's or college's staff behaviour policy (sometimes known as a code of conduct). This policy should amongst other things include acceptable use of technologies, staff pupil/student relationships and communication including the use of social media. The policy should apply equally to any existing or new online and distance learning arrangements which are introduced. Schools and colleges should, as much as is reasonably possible, consider if their existing policies adequately reflect the new reality of so many children (and in some cases staff) working remotely online. As with the child protection policy, in some cases an annex/addendum summarising key COVID-19 related changes may be more effective than re-writing/re-issuing the whole policy. The principles set out in the guidance for safer working practice for those working with children and young people in education settings published by the Safer Recruitment Consortium may help schools and colleges satisfy themselves that their staff behaviour policies are robust and effective. In some areas schools and colleges may be able to seek support from their local authority when planning online lessons/activities and considering online safety.

Schools and colleges should ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school or college this should also signpost children to age appropriate practical support from the likes of:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Parents and carers may choose to supplement the school or college online offer with support from online companies and in some cases individual tutors. In their communications with parents and carers, schools and colleges should emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children. Support for parents and carers to keep their children safe online includes:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and careers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers

The department encourages schools and colleges to share this support with parents and carers.

Writing and reviewing the online safety policy

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

- Safeguarding and Child Protection Policy
- Behaviour Policy and Practice
- Anti-Bullying Policy and Practice
- Computing Policy
- PSHE Policy (and RSHE Policy)
- Data Protection Policy
- Social Media Policy
- Remote Education Policy

2020-21 arrangements

Designated Safeguarding Lead
Cheryl Payne – Head Teacher

Deputy Designated Safeguarding Lead
Amanda Bishop – Deputy Head Teacher
Kerry Dunford – Inclusion Manager

Online Safety Coordinators
Mark Lett - Computing Subject Leader
Monica Read - Computing Support

Our Online Safety Policy has been written by the school, building on Wandsworth's Safeguarding Children Boards' e-Safety Policy, LGfL's online safety policy and government guidance. It has been agreed by all staff and approved by governors.

The Online Safety Policy 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	January 2018	-	January 2019
Mr Mark Lett	June 2019	June 2019	June 2020
Mr Mark Lett	May 2020	-	May 2021
Mr Mark Lett	May 2021	May 2021	May 2022

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: 2021-2022

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:

APPENDIX C

Acceptable Use Policy – Staff Agreement

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, digital learning platforms and cloud storage environments, e-mail, software, hardware, equipment, hand held devices and other new digital and electronic technologies.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the head teacher and Governing Body.
- 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 not engage in any online activity that may compromise my professional responsibilities.

- 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 and the internet, including social media.

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

- 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 browse, download or send material that could be considered offensive or of an extremist nature by the school.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.

- 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 head teacher 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 never use school devices and networks / internet / digital learning 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 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 alert the school's designated safeguarding lead / named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated safeguarding lead / named child protection officer / relevant senior member of staff.
- 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.
- I understand that all school internet, network, device and digital learning platform usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

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 policy.

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.

Signature: _____ Date: _____

Authorised Signature

Full Name: _____ (printed)

Job title: _____

I approve this user to be set up.

Signature: _____ Date: _____

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?

LGfL DigiSafe
Keeping children safe

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

@LGfLDigiSafe

*** Need templates?**
See safepolicies.lgfl.net

APPENDIX D

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