FOUNDED 1789

St. Mary’s Church of England Primary School

Online Safety Policy

Date: January 2024

Reviewed and Ratified by Governing body on 20 March 2024

Review Date: January 2027

Signed : ________________________ Rev’d Melissa Carter, Chair of Governors

Signed : ________________________ Helen Comfort, Executive Headteacher

Equality

We recognise our duty and responsibility to establish equality for all pupils, staff, other members of the school community and service users regardless of their ethnicity, gender, disability, sexual orientation, age or beliefs as defined within existing equalities legislation (please see ‘Single Equality Scheme’).

1.1 Aims and policy scope

St. Mary’s Church of England Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

St. Mary’s Church of England Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

St. Mary’s Church of England Primary School has a duty to provide the school community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions. St. Mary’s Church of England Primary School also identifies that with this there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of St. Mary’s Church of England Primary School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that St. Mary’s Church of England Primary School is a safe and secure environment.
- Safeguard and protect all members of St. Mary’s Church of England Primary School community online.
- Raise awareness with all members of St. Mary’s Church of England Primary School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as ‘staff‘ in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality and relevant curriculum policies.

1.2 Writing and reviewing the online safety policy

St. Mary’s Church of England Primary School online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.

The policy has been approved and agreed by the Leadership Team and Governing Body.
The school has appointed the Designated Safeguarding Lead (Matthew Lamprell) as an appropriate member of the leadership team and the online safety lead.

The online safety (e–Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

The Designated Safeguarding Lead (DSL) is Matthew Lamprell (Head of School)
The Online safety (e-Safety) lead for the Governing Body is Nigel Simmons.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the school/setting management and leadership team are:

Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.

Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.

Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.

Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.

To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.

To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.

Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.

Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.

Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.

To ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.

Keeping up-to-date with current research, legislation and trends regarding online safety.

Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

To work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.

Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.

To monitor the school's online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need

To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.

Liaising with the local authority and other local and national bodies, as appropriate.

To review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.

Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

Contributing to the development of online safety policies.

Reading the school Acceptable Use Policies (AUPs) and adhering to them.

Taking responsibility for the security of school/setting systems and data
.
Having an awareness of a range of different online safety issues and how they may relate to the children in their care.

Modelling good practice when using new and emerging technologies.

Embedding online safety education in curriculum delivery wherever possible.

Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.

Knowing when and how to escalate online safety issues, internally and externally.

Being able to signpost to appropriate support available for online safety issues, internally and externally.

Maintaining a professional level of conduct in their personal use of technology, both on and off site.

Demonstrating an emphasis on positive learning opportunities.

Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.

Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.

To report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.

Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

1.3.5 The key responsibilities of children and young people are:

Reading the school's setting Acceptable Use Policies (AUPs) and adhering to them.

Respecting the feelings and rights of others both on and offline.

Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

Reading the school’s Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

Role modelling safe and appropriate uses of technology and social media.

Identifying changes in behaviour that could indicate that their child is at risk of harm online.

Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).

The contact details on the website will be the school address, email and telephone number. Staff or pupils’ personal information will not be published.

The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

The administrator account for the school website will be safeguarded with an appropriately strong password.

The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

The school will ensure that all images and videos shared online are used in accordance with the school image use policy.

The school will ensure that all use of images and videos take place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.

In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

All members of staff are provided with a specific school email address to use for any official communication.

The use of personal email addresses by staff for any official school business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and password protected email.

Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.

Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Appropriate and safe classroom use of the internet and any associated devices

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.

The school/'s internet access will be designed to enhance and extend education.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability.

- At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will use age appropriate search tools.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Media Policy

3.1. General social media use

Expectations regarding safe and responsible use of social media will apply to all members of St. Mary's Church of England Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

All members of St. Mary's Church of England Primary School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

Information about safe and responsible use of social media will be communicated clearly and regularly to all members of St. Mary's Church of England Primary School community.

All members of St. Mary's Church of England Primary School community are advised not to publish specific and detailed private thoughts, opinions/concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The school will block pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.

The use of social networking applications during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.

Any concerns regarding the online conduct of any member of St. Mary's Church of England Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

St. Mary's Church of England Primary School official social media channels are: Facebook (in progress).

Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.

Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.

Staff will use school provided email addresses to register for and manage any official approved social media channels.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Any online publication on official social media sites will comply with legal requirements including the UK GDPR supported by the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
Official social media use will be in line with existing policies including anti-bullying and child protection.

Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.

Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.

Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.

Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.

Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.

The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.

All members of staff are advised not to communicate with or add as ‘friends’ any current or past children/pupils or current or past pupils’ family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels

Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies (safeguarding, child protection, data protection etc.) and the wider professional and legal framework.

Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

Members of staff are encouraged not to identify themselves as employees of St. Mary’s Church of England Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.

Members of staff will ensure that they do not represent their personal views as that of the school on social media.

School email addresses will not be used for setting up personal social media accounts.

3.4 Staff official use of social media

If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.

Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.

Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

Staff using social media officially will sign the school/setting social media Acceptable Use Policy.

3.5 Pupil use of social media

Safe and responsible use of social media sites will be outlined for Upper Key Stage 2 pupils and their parents as part of the Acceptable Use Policy.

Personal publishing on social media sites will be taught to Upper Key Stage 2 pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

Upper Key Stage 2 Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult’s permission and only when they can be present.

Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices (which may also include smart technology) among children, young people and adults will require all members St. Mary’s Church of England Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use Policy.

St. Mary’s Church of England Primary School recognises that personal communication through mobile and smart technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices, mobile phones and smart technology

All use of personal devices and mobile phones and smart technology will take place in accordance with the law and other appropriate school policies.

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.

Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.

All members of St. Mary’s Church of England Primary School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of St. Mary’s Church of England Primary School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

All members of St. Mary’s Church of England Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.

School mobile phones and devices must always be used in accordance with the Acceptable Use Policy.

4.3 Pupils use of personal devices, mobile phones and smart technology

Pupils are not permitted to bring mobile ‘phones or personal devices with smart technology to school or on school trips.

Upper Key Stage 2 Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and personal devices, and will be made aware of behavior expectations and consequences of policy breaches.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school/setting ‘phone.

Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

School staff may confiscate a pupil’s mobile phone or device if they are known to have it with them at school or on a school trip. If staff believe the ‘phone being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting), the phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the DfE advice on Searching, Screening and Confiscation.

If there is suspicion that material on a pupil’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices, mobile phones and smart technology

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Members of staff will ensure that any use of personal phones, smart technology and devices will always take place in accordance with the law e.g. data protection as well as school policy and procedures

Staff personal mobile phones and devices will be switched off/switched to ‘silent’mode and kept out of sight during lesson times.

Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.

Personal mobile phones, smart technology or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.

Staff will ensure that any content brought on site via mobile phones, smart technology and personal devices are compatible with their professional role and expectations.

Personal USB sticks or portable hard drives are not be brought on site or used on the school network.

If a member of staff breaches the school policy then disciplinary action will be taken.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

Any allegations against members of staff involving personal use of mobile phone, smart technology or devices will be responded to following the school allegations management policy.

4.5 Visitors use of personal devices, mobile phones and smart technology

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

St. Mary's Church of England Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.

The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.

5.2 Authorising internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.

All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.

Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

Pupil’s input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.

Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.

All users will be informed that network and Internet use will be monitored.

Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.

Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.

Acceptable Use expectations and Posters will be posted in all rooms with Internet access.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

External support will be used to complement and support the school’s internal online safety (e-Safety) education approaches.

6.2 Engagement and education of children and young people considered to be vulnerable

St. Mary’s Church of England Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors.

St. Mary’s Church of England Primary School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.

Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

St. Mary's Church of England Primary School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters and on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Information and guidance for parents on online safety will be made available to parents in a variety of formats.

Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2 Security and Management of Information Systems

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

Unapproved software will not be allowed in work areas or attached to email.

Files held on the school's network will be regularly checked.

All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

All users will be informed not to share passwords or information with others and not to login as another user at any time.

Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.

All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

7.3 Filtering and Monitoring

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

St. Mary's CEP (VA) School will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.

It is important to recognise that no filtering systems can be 100% effective and need to be supported by good teaching and learning practice and effective supervision.

The school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils and is in line with the requirements of the Prevent duty and KCSIE.

The school uses Smoothwall filtering system which meets the national defined 'appropriate filtering standards' and is certified by the UK Safer Internet Centre.

We work with Cantium and our IT service providers/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

Parents/carers will be informed of filtering breaches involving their child.

Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.

All monitoring of school owned/provided systems will take place to safeguard members of the community.

All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:

- Effective physical supervision of the pupils while they are using the school devices
- Receiving regular smoothwall safeguarding alert notifications which will send safeguarding breaches levelled 1-5 (5 being severe)
- Checking the different staff and pupil group configurations are effective

If a concern is identified via our monitoring approaches:

- Where the concern relates to pupils, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.

- Where the concern relates to staff, it will be reported to the Executive Headteacher (or chair of governors if the concern relates to the Executive Headteacher), in line with our staff behavior/ allegations policy.

Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.

8. Responding to Online Incidents and Safeguarding Concerns

All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.

Any complaint about staff misuse will be referred to the head teacher.

Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Pupils, parents and staff will be informed of the schools complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concern as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.

Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School’s complaints procedure.

Complaints about online bullying will be dealt with under the School’s anti-bullying policy and procedure.

Any complaint about staff misuse will be referred to the headteacher.

Any allegations against a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).

Where there is a data incident this will be logged on GDPRiS (where we they will receive an alert) and in the case of a serious breach inform the DPO directly for advice and guidance ASAP.

Pupils, parents and staff will be informed of the school’s complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.

Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- If a Kent child is at risk of imminent harm, call the Integrated Front Door on 03000 411 111 (outside office hours - 03000 419 191) or the Police on 999.
- onlinesafety@theeducationpeople.org

Kent Police:
www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net
Kent Safeguarding Children Board (KSCB): www.kscb.org.uk
Kent e–Safety Blog: https://www.theeducationpeople.org/blog/
Cantium: ICT Support for Schools and Kent Schools Broadband Service Desk**:**
https://cantium.service-now.com/

National Links and Resources

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

Appendix B

Acceptable Use Policy (AUP) for Remote Learning and Online Communication

St. Mary's Church of England Primary School Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguard all members of St. Mary's Church of England Primary School community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. The School will publish weekly curriculum planning on the school website. When required, the school will make use of the National Oaks Academy and BBC Bitesize recorded lessons.

2. Staff will only use school managed professional email accounts with learners and/or parents/carers
   - Use of any personal emails accounts to communicate with learners and/or parents/carers is not permitted.
     - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment e.g. a school/setting laptop, tablet, or other mobile device.

3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:
   - Monday to Friday 8am to 5pm term-time only

Data Protection and Security

4. Any personal data used by staff and captured by email when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
   - Email to multiple users (e.g. whole year groups) will be achieved using bcc to email.

5. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the staff Code of Conduct.

6. Staff will not record lessons or meetings using personal equipment.

7. Only members of school office will be given administrator rights to access the school website.

8. Access to the school website and emails will be managed in line with current IT security expectations as outlined in the Online Safety Policy.

9. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

Sample Letter for parents/carers

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to: [this list is not exhaustive]

- Computers, tablets and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones

St. Mary's Church of England Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the school's safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. However no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the school internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety (e-Safety) policy are available on the school website or on request.

We request that all parents/carers support the school's approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact me.

(Additional Paragraph for Early Years/KS1/SEN)
We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely, Headteacher

FOUNDED 1789

Pupil Acceptable Use Policy

EYFS and KS1 shortened version

□ I only go online with a grown up present

□ I only use the apps/programmes my teacher tells me to use

□ I am kind online

□ I keep information about me safe online

□ I tell a grown up if something online makes me unhappy or worried

Statements for Early Years and KS1 (0-7)

□ I only use the internet when an adult is present

□ I only click on links and buttons when I know what they do. If I am not sure, I will ask an adult.

□ I will not assume information online is true

□ I know that people online are strangers, and they may not always be who they say they are

□ I keep my personal information and passwords safe online

□ I will not use technology to be unkind to people

□ I know the school can see what I am doing online when I use the school computers and tablets

□ I have read and talked about these rules with my parents/carers

□ I always tell an adult/teacher if something online makes me feel unhappy or worried

□ I can visit www.thinkuknow.co.uk to learn more about keeping safe online

Statements for KS2 Pupils (7-11)

□ I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.

□ I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.

□ I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.

□ I know that people online are strangers, and they may not always be who they say they are

□ I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.

□ I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.

□ If I get unpleasant, rude or bullying emails or messages I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.

□ I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.

□ I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.

□ I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.

□ I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.

□ If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.

□ I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

□ I know I am not to use my mobile phone at school or take it on school trips.

□ If I need to learn online at home, I will follow the school remote learning Acceptable Use Policy

□ I know I can visit www.thinkuknow.co.uk; www.childnet.com and www.childline.org.uk to find out more about keeping safe online

FOUNDED 1789

Pupil Acceptable Use Policy
Parent/Carer Acknowledgement Form

Pupil Acceptable Use Policy – St. Mary's Church of England Primary School Parental Acknowledgment

I, with my child, have read and discussed St. Mary's Church of England Primary School Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the schools systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I understand that the AUP applies to my child's use of school devices and systems on site and at home where there are any safeguarding and/or behaviour concerns. This may include if online behaviour causes harm to another person, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school, of if the behaviour could adversely affect the reputation of the school.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I am aware that the school policy states that my child cannot use personal mobile phones, smart technology and devices on the school site.

I will support the schools online Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

I understand that there may be a need for my chid to have a safe and appropriate place to access remote learning, for example if the school is closed in response to Covid 19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school's Remote Learning Acceptable Use Policy.

Child's Name……………………………………………… Signed …………………………………..

Class…………………………   Date……………………..

Parents Name…………………………………………......Parents Signature…………………………

Date…………….

FOUNDED 1789

St. Mary’s Church of England Primary School Staff

Acceptable Use Policy 2024

As a professional organisation with responsibility for children’s safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school’s computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a ‘strong’ password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (staff laptops and use of email) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. Where I deliver or support remote learning, I will comply with the school's Remote Learning Acceptable Use Policy.

8. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the VPN portal to upload any work documents and files. I will protect the devices in my care from unapproved access or theft.

9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

10. I will respect copyright and intellectual property rights.

11. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices and smart technologies, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

12. I will report all incidents of concern regarding children's online safety in line with the school's Child Protection Policy to one of the Designated Safeguarding Leads (Matthew Lamprell, Helen Comfort, Louisa Wallis or Debra Morris) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to one of the Designated Safeguarding Leads (Matthew Lamprell, Helen Comfort, Louisa Wallis or Debra Morris) as soon as possible.

13. I will report concerns about the welfare, safety, or behaviour of staff online to the Executive Headteacher, in line with the school's Child Protection Policy and/or the allegations against staff policy.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Business Manager (Lorraine Windsor) as soon as possible.

15. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

16. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

17. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

18. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

19. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the one of Designated Safeguarding Leads (Matthew Lamprell, Helen Comfort, Louisa Wallis or Debra Morris).

20. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. Monitoring will be conducted via regular audit and be compliant with current data protection and privacy legislation.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ………………………... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: …………………………

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

Schools/settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. Schools may choose to require that visitors agree to an on screen electronic AUP as part of the process of accessing the Wi-Fi. This template is provided for schools to adapt and use as appropriate.

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The school provides Wi-Fi for the school community and allows access for education and administration uses only.

The use of ICT devices falls under St. Mary's Church of England Primary School's Acceptable Use Policy, online safety (e-Safety) policy, Child Protection and behaviour policy which all pupils/students/staff/visitors and volunteers must agree to, and comply with.

1. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

2. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software, systems updates).

4. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

5. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to,

viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

6. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

7. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

8. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.

9. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

10. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

11. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead and Online Safety Lead (Matthew Lamprell), as soon as possible.

12. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Lead (Matthew Lamprell) or the Executive Head Teacher (Helen Comfort).

13. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with St. Mary's Church of England Primary school Wi-Fi Acceptable Use Policy.

Signed: ……………………….... Print Name: ……………………… Date: ………

Accepted by: …………………………… Print Name: ………………………….

FOUNDED 1789

Staff Social Networking Acceptable Use Policy

For use with staff running official school social media accounts

1. As part of the school’s drive to encourage safe and appropriate behaviour in the use of today’s technology, I will support the school’s approach to Online safety (e-Safety) . I am aware that the tool using e.g. Facebook, Twitter is a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the site/page to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

3. I will follow the school’s policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on (tool using e.g. Facebook, Twitter) and will not be forwarded to any other person or organisation.

4. I will promote online safety (e-Safety) in the use of (tool using e.g. Facebook, Twitter) and will help to develop a responsible attitude to safety online and to the content that is accessed or created..

5. I will set up a specific account/profile using a school provided email address to administrate the account/site/page (tool using e.g. Facebook, Twitter) and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the tool using Facebook and Twitter.

6. Where it believes unauthorised and/or inappropriate use of the tool using e.g. Facebook, Twitter or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

8. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

I have read and understood and agree to comply with the School Social Networking Acceptable Use policy.

Signed: ……………………..... Print Name: …………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….