Headteacher:
Mrs M. Constantinou BEd
Littlegrove, East Barnet, Herts EN4 8SR
t: 020 8449 5856
e: office@stmarysen4.barnetmail.net
www.stmarysen4-barnet.co.uk

Ofsted Outstanding 2009|2010

learning in faith in

St Mary's
Church of England Primary School

ONLINE SAFETY POLICY 2022

VISION

At St Mary's, inspired by Christian values, we are excited by our learning, proud of our achievements, determined to be the best we can be and caring of all of God's creation'.

VISION IN CHILD SPEAK

Inspired by Christian values, I am excited about my learning, proud of my achievements, determined to be the best I can be and caring of all of God's creation.

MISSION

- Through excellent teaching we will deliver an inspirational curriculum
- We will enable every child to make the very best progress
- We will work in partnership with children and families to further promote confidence and self esteem
- We will prepare children to confidently face the challenges of growing up in the 21st Century
- We will provide children with an understanding of local, national and global communities and faiths
- With St Mary's Church, Brookside Methodist, and other local churches we will further develop understanding of gospel values in action through worship and across the curriculum

Safeguarding Statement of Intent

St Mary's Church of England Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. Every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm to their mental or physical health or development. This is the responsibility of every adult employed by or invited to deliver services at to the school. We recognise our responsibility to safeguard and promote the welfare of all our pupils by protecting them from physical, sexual or emotional abuse, neglect and bullying. St Mary's Church of England Primary School is committed to safeguarding and promoting the welfare of children and young people through rigorous application of Safer Recruitment processes. All applications for staff positions in the school are thoroughly vetted in accordance with policy. DBS checks are undertaken for all staff and for volunteers who work on a regular basis in school.

Approved by:	Full Governing Body	**Date:** March 2022
Last reviewed on:	March 2021	
Next review due by:	March 2023	

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating pupils about online safety in school and during remote learning 4
5. Educating parents about online safety 5
6. Cyber-bullying and Cyber-crime 6
7. Acceptable use of the internet in school 7
8. Pupils using mobile devices in school 7
9. Staff using work devices outside school 7
10. How the school will respond to issues of misuse 7
11. Training 8
12. Monitoring arrangements 8
13. Links with other policies 8
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 9
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 10
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 11
Appendix 4: useful links for parents and carers - staying safe online at home 12

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteachers to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding leads

Details of the school's DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and safeguarding policy where appropriate
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Computing leader

The Computing leader is responsible for:

- Working with senior staff to put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Working with senior staff to ensure that the school's online systems and devices are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Working with senior staff to ensure that potentially dangerous sites are blocked and, where possible, prevent the downloading of potentially dangerous files
- Working with senior staff to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Working with senior staff to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteachers of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? - UK Safer Internet Centre
    - Hot topics - Childnet International
    - Parent factsheet - Childnet International
    - Healthy relationships – Disrespect Nobody
    - Safe internet use – ThinkUKnow
    - Online Safety guides - NSPCC

Additional useful links can be found in appendix 4.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety in school and during remote learning

Pupils will be taught about online safety as part of the curriculum:

In **EYFS and Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Managing 'screen time'
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant e.g. within the PSHE and Sex, Health and Relationships curriculum.

Online safety: Remote Learning

The use of the online learning platform Google Classroom has developed since the Covid-19 pandemic. This platform is in use for home learning and for children to access learning in the event of Covid self-isolation.

In the event of any class/school enforced closures, Google Classroom becomes the only platform for learning in the absence of being in school. Children are expected to behave online in accordance with live classroom behaviour. The following measures are in place to ensure that children are not exposed to risk during remote learning.

- In any live Google Meet, the children must be in a communal area of their home and never in their bedroom. They must always be appropriate dressed and typically wear a school shirt. Google Meets are never recorded and the teacher is always the host so that they have full control, including the ability to disable the chat if needed. Staff are also advised to position themselves in a neutral space during a live Google Meet and to dress as if they were on site.
- Google Classroom is closely monitored by the teacher, particularly the Stream. Children are reminded that comments should be focused on learning. If any inappropriate comments are made, they will be deleted immediately and parents will be notified.
- Children know that they must never post photos or videos of themselves on the Stream. Should this occur, teachers will remove and contact parents directly to notify them.
- Our Google Drive as part of G Suite for Education, is only visible to users at St Mary's.
- Any YouTube videos created by staff are 'unlisted' so that only people who have the link will be able to see the video. The audience is set as 'made for kids', so that adverts don't appear at the start of the video, and comments are disabled.
- Where multiple online videos are shared e.g. in our virtual library, YouTube links are converted to Video Links so that no further online content can be explored in that location.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on the website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteachers and/or the DSLs.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

The school will host cyclical online safety workshops for parents and carers over time.

6. Cyber-bullying

6.1 Cyber-bullying definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also shares information on cyber-bullying with parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSLs will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Cyber-crime definition

Cyber-crime is defined as criminal activity carried out by means of computers or the internet.

6.4 Preventing and addressing cyber-crime

We will ensure that pupils in upper Key stage 2 understand what it is and what to do if they become aware of it happening to them or others. Children learn about importance of not sharing personal information online from EYFS and they develop their understanding of keeping log in details private and secure as they enter Key Stage 1. In upper Key Stage 2 the computing curriculum ensures that children are made aware of online scams, hacking and phishing messages that come in the guise of texts or emails relating to this.

6.4 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSLs or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices to school (e.g. if there are independent travellers), but are not permitted to use them in school. All devices are handed to a member of staff.

Pupils may wear smart watches in school but should not wear devices capable of taking photographs or video footage.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policy on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Computing lead and Headteacher. At every review, the policy will be shared with the governing body.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use documentation
- Relationships, Sex and Health education policy
- Anti-Bullying

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's IT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • I will be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's IT systems (like computers) and get onto the internet in school I will:** • Always use the school's IT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it in school. It will only have it on site of I am travelling to and from school on my own. • I will hand it to an adult for safe keeping when I arrive and collect it at home time. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with the teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
• I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Useful links for parents and carers – staying safe online at home

https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Online safety advice
Inappropriate and sexual behaviour
Worried about something online?
Online safety guides for parents

https://www.digitalparentingcoach.com/
Critical thinking and positive influence on YouTube
Advice regarding sexual content in games

https://www.internetmatters.org/parental-controls/
Parental controls and privacy settings

https://parentsafe.lgfl.net/#h.kiustevr44ys
Top tips for parents right now!
Safe settings, controls & monitoring
What's that app anyway?
Talking to children about life online
Screen time
Help & reporting

https://www.taminggaming.com/
Search for general information about games

https://support.google.com/youtube/answer/10314074?hl=en&ref_topic=10314939
YouTube support for setting up supervised accounts and filters

https://www.internetmatters.org/resources/online-gaming-advice/?utm_source=Parents+Newsletter&utm_campaign=56b5b81091-EMAIL_CAMPAIGN_Jan_13_2022_Parents_COPY_01&utm_medium=email&utm_term=0_290cc150e6-56b5b81091-386150004
Online gaming advice
Dangers of some online games

https://saferinternet.org.uk/online-issue
Misinformation
Sexting
Social media
Online challenges
Parental controls
Gaming
Online bullying

https://www.commonsensemedia.org/
Reviews, dangers, age ratings for games, apps, films and TV shows.
Parent guides to filters, privacy settings, games, apps and phones

Childrens-Commissioners-Office-Talking-to-Your-Child-About-Online-Sexual-Harassment-A-Guide-for-Parents.pdf (internetmatters.org)
Advice on difficult conversations with children