"I am the way, the truth, and the life." (John 14:6)

St Mary's is a Catholic Primary School.
We place our children at the heart of all we do,
inspired by the love, life and teachings of Jesus
and the Catholic Christian Church.

Online Safety Policy

This policy should be read in conjunction with Acceptable use of the internet policies, ICT policy, Child-Protection and Safeguarding, Tackling Extremism and Radicalisation, Data Protection, Mobile Phone and Anti- Bullying Policies.

Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction.
- We recognise that we have a duty to provide children with quality Internet access as part of their learning experiences.
- Internet use is a part of the curriculum and an integral tool for learning.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering using Netsweeper software.
- Pupils will be taught what Internet use is acceptable and what is not and given the responsibility of working within these expectations.
- Pupils will be educated in the effective use of the Internet to support their learning. This will be through an age-appropriate, progressive digital literacy curriculum.

Curriculum

Online safety education is an integral part of our curriculum will be provided in the following ways:

- A planned digital literacy programme is provided as part of the Computing Curriculum and is regularly revisited, covering both the use of ICT and new technologies in and outside of school.
- Digital literacy will be taught explicitly at the beginning of each topic and then reinforced as necessary across the curriculum.
- Through the planned curriculum the children will be taught to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Key online safety messages are reinforced as part of a planned programme of assemblies and through PSHE circle time activities in classes.
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of

information
- Children should be helped to understand the need for the pupil acceptable use policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT, the network and the internet will be posted in all classrooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Online safety should be a focus in all areas of the curriculum and all staff have a responsibility to reinforce online safety messages in the use of ICT across the curriculum.

- In the EYFS and KS1 it is best practice that children should be guided to sites checked as suitable for their use.
- Children in KS2 are taught to use the internet for research purposes. They are taught search techniques to ensure that the search returns the most reliable results. The safe search option is enabled on all forms of technology accessible to the children.
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of any information
- Children should be taught to acknowledge the source of information used and to respect copyright when using information and material from the internet.

If children were to access information that was inappropriate the procedure is as follows

- Turn over the iPad or switch off the computer screen
- Tell a trusted adult immediately
- A member of staff to view the screen and complete an online-safety incident report form, recording the exact web address, see Appendix 1
- The form is passed to Susan Buscombe, the online safety lead and in her absence to Jacqui Scarborough, the designated safeguarding lead. In the unlikely event that neither are available log the incident with NCi via email to help@ncitech.co.uk
- The issue will be investigated by NCi and passed onto Netsweeper, as deemed necessary.
- An update on the progress of the issue will be given to the class teacher, the children involved and parents, as deemed appropriate

Education – Parents

Parents and carers may have an essential role in the continuing education of their children and in monitoring their online experiences. Parents may underestimate how often children may come across inappropriate material on the internet and are often unsure about what they would do about it.

The school will seek to provide information to parents and carers through:

- Letters
- Newsletters
- Website
- Parent information meetings

Education & Training – Staff and Governors

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- Online safety forms part of the induction process for all new staff. They will be given online safety training, delivered in house by the online safety lead.
- An audit of the online safety training needs of all staff will be carried out regularly.
- The online safety lead will receive regular updates through attendance at training sessions and by reviewing guidance documents released by Naace, Swgfl, Ofsted and the DfE.
- This online safety policy and its updates will be presented to and discussed by staff in professional development meetings. An annual update is provided for all staff, in conjunction with regular updates to policy and practice.
- The online safety lead will provide advice, guidance and training to individuals as required
- All staff are expected to sign an acceptable use policy annually

Through our comprehensive training and support we aim that

- All adults understand the risks posed by adults or learners who use technology, including the internet, to bully, groom, radicalise or abuse children or learners.
- They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe.

Leadership and Management

We have a designated online safety leader in school who works closely with the designated safeguarding lead to ensure the safety of all members of the school community.

Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being.

Leaders and managers are aware of the potential issues with the safe use of electronic and social media by staff and learners and take action immediately if they are concerned about bullying or risky behaviours. Advice is given to staff as part of the induction process and through ongoing staff training.

The governing body have a strategic role in developing our online safety provision. There is a designated online safety governor and all governors receive up to date training at least annually, delivered in-house by our online safety lead.

Technical – infrastructure / equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements as outlined in the latest online safety guidance and the current Ofsted guidance. We ensure that our systems and

procedures comply with the GDPR legislation.

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Any network changes should be discussed with the ICT subject leader, before any changes are made. The Apple management system has been set with three levels of access, pupils, staff and administrators.
- The school maintains and supports the managed filtering service provided by Netsweeper.
- Teaching staff will have access to the Netsweeper proxy to enable them to unblock a specific site for a teaching session.
- It is the responsibility of the member of staff to check the content of any sites that they use in school.
- It is important that the Netsweeper proxy password is not shared with pupils. If a member of staff thinks that the password may have been compromised this should be reported to the online safety lead and/or the Headteacher as soon as possible.
- Any global changes to the filtering policies can only be undertaken by members of staff with the management access rights. The named members of staff who can make global changes are Jacqui Scarborough, Headteacher, and Susan Buscombe, Online Safety leader. When making any global changes to the filtering system the relevant form must be completed, indicating the reasons for the change and signed. It will then be passed to the online safety lead and filed. See Appendix 2
- Any filtering issues should be reported immediately to the online safety lead and/or the Headteacher. When necessary these issues will be escalated to Netsweeper via NCI
- School ICT technical staff and the Headteacher may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Any potential or actual online safety issues will be reported to the online safety lead or the Headteacher
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. .
- An agreed policy is in place regarding the use of removable media by users on school workstations / portable devices. Removable media should only be used on the school network where up to date virus protection can be ensured. USB sticks that contain personal data of pupils and/or staff must be encrypted to ensure that we are complying with the GDPR legislation.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or password protected.
- The online safety lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet such as on social networking sites.
- Staff are encouraged to take digital and/or video images to support teaching and learning, but must follow school policies concerning the sharing, distribution and publication of those images. Staff should ensure that images of children are only taken on encrypted and/or password protected devices.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website and the school Facebook page that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Childrens' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or on the school Facebook page.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (GDPR) which states that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Kept in a form which permits identification for no longer than is necessary.
- Processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Use their school provided laptop to store any personal data and that this is encrypted and only accessed via a password.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be encrypted and/or password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Published content and the school web site and Facebook page

The contact details on the website and Facebook page will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. Only staff may publish content on the school website and Facebook page. Parents and visitors may comment on Facebook posts but are unable to post to the page.
The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include children will be selected carefully.
- Childrens' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of children are published on the school website and Facebook page. A complete list of those pupils with parental permission is kept in the school office. Class teachers retain a copy of those lists relevant to their class.

Social networking and personal publishing

- The school will block/filter access to social networking sites unless a specific use is approved.
- Children will be taught never to give out personal details of any kind which may identify them or their location
- Children are taught not to place personal photos on any social network space.
- Children are advised on security and encouraged to set passwords, and taught how to block and report unwanted communications.
- Children and parents will be advised that the use of many social network spaces outside school is inappropriate for primary aged pupils. They will be taught about the age restrictions of common social networking sites.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning
When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and children are able to use the school email service to communicate electronically with others when in school
- Staff and children need to be aware that email communications may be monitored
- Staff and children must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Teachers and children may communicate electronically via their Showbie accounts. The class discussions are available only to those children in the class and are considered safe and secure. Children are taught to use the discussion

forum in a polite and respectful manner.

- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class, group or individual email addresses will be used, for educational use.
- Children should only bring mobile phones into school in accordance with the school policy. The phone will be handed to a member of school staff to be kept securely during the school day.

Password Security

- Password security is essential for staff, particularly as they are able to access and use pupil data. All staff are expected to have secure passwords which are not shared with anyone.
- The children are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and children are regularly reminded of the need for password security.
- Children are provided with a class network username. Staff members have a network, e-mail, and SIMS password.
- If a password may have been compromised or someone else has become aware of the password it must be changed as a matter of urgency. Advice may be sought from the ICT lead as needed.
- All staff are aware of their individual responsibilities to protect the security and confidentiality of school networks.

Sexting

St Mary's School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating child produced sexual imagery (known as "sexting"). We view "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead

The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'

If the school are made aware of incident involving child produced sexual imagery the school will:

- Act in accordance with the schools Child protection and Safeguarding policy
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.

- The school will not view any images suspected of being child produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead and a senior member of staff).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.
- We will take action regarding creating child produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- We will ensure that all members of the community are aware of sources of support regarding child produced sexual imagery

Review and Monitoring

As a school we use the 360° Safe to review our online safety policies and practices. The review framework is updated at least termly and action plans are generated to inform our practice. This framework can be accessed through www.360safe.org.uk/

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Any incidents of misuse will be reported to the Headteacher and/or the online safety lead.

Policy Prepared by Susan Buscombe
Reviewed September 2017
To be reviewed annually, by September 2018

Appendix 1

Online Safety Incident Log

Date/Time:
Details of incident:
Who was involved:
Reported to:
Action taken:
Follow up actions required:

Appendix 2

Request for global access to an internet site

Date
Member of staff
URL of website
Reason/ Educational use
Action taken:
Actioned by: