St. Matthew's
Church of England
Primary School

Online Safety Policy

Our Vision is

‘ to enable our whole school community to live life in all its fullness.’

This school is committed to safeguarding and promoting the welfare of our children and this policy supports this commitment.

Date: Spring 2019

Review Date: Summer 2021

St. Matthew's
C of E Primary School

Online Safety Audit

Has the school an online safety policy	Yes
Date of latest update :	Jan 19
The policy is available for staff at:	Staff meeting, School Website
The policy is available for parents/carers at:	School website
The responsible member of the Senior Leadership Team is:	Clare Taylor
The responsible member of the Governing Body is:	Robin (C of G)
The Designated Child Protection Coordinator is:	Clare Taylor
The Online Safety Coordinator is:	Clare Taylor / Nicola Tuck
Has online safety training been provided for both pupils and staff?	Staff – Yes regular updates at staff briefing and staff meetings Pupils –.Yes. Online safety is imbedded throughout the curriculum, as well as taught explicitly to all year groups during online safety units. As a school we take part in 'Safer Internet Day' (February 2019) where every year group spend the day learning about online safety, as well as attending Key Stage Assemblies about online safety. ChildNet training with pupils in Y2,4,6 ChildNet training for teachers in staff meeting ChildNet training for parents in twilight workshop.
Is there a clear procedure for a response to an incident of concern?	Yes – via Pam Dryden / Clare Taylor
Do all staff sign a Code of Conduct for ICT on appointment?	Yes
Are all pupils aware of the School's online-safety rules?	Yes
Are online-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Yes
Do parents/carers sign and return an agreement that their child will comply with the school online-safety rules?	Yes, on entry to school
Has an ICT security audit been initiated by SLT, possibly using external expertise?	LGfl filtering
Is personal data collected, stored and used according to the principles of GDPR 2018?	Yes
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements	Yes – LGfL - Atomwide
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	Yes – LGfl - Atomwide

Online-safety policy

The online-safety policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
The school has appointed an Online - Safety Coordinator to deal with any issues that may arise.

Our Online-Safety Policy has been written by the school, building on LA and government guidance.

It has been agreed by senior management and approved by governors.

This Online-Safety Policy was written by the Computing Coordinator
The next review date is: Jan 2020

Teaching and learning

Why the Internet and digital communications are important?
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning
The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
Pupils will be shown how to publish and present information to a wider audience.
Pupils in KS2 will be taught about how the internet works

Pupils will be taught how to evaluate Internet content
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils will be taught the importance of cross-checking information before accepting its accuracy.
Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Information system security
School ICT systems security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be in line with the Local Authority guidance.

E-mail
Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive an offensive e-mail.
In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
The school should consider how e-mail from pupils to external bodies is presented and controlled.
The forwarding of chain letters is not permitted.

Published content and the school web site
Staff or pupil personal contact information will not generally be published. The contact details given online are for the

school office.
The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work
Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. We will use photographs rather than full-face photos of individual children.
Pupils full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
Work can only be published with the permission of the pupil and parents/carers.
Pupil image file names will not refer to the pupil by name.
Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing
The school filtering system does not allow control access to social networking sites at present. This is currently under discussion by the LA.
Newsgroups will be blocked
Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
Pupils and parents will be advised that the use of social network spaces outside of school brings a range of dangers for primary aged pupils.
Pupils will be advised to use nicknames and avatars if using such sites.

Managing filtering
The school will work with the LA to ensure systems to protect pupils are reviewed and improved.
If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online-Safety Coordinator. &/or Computing Coordinator
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing & webcam use
Video conferencing is not currently available to our pupils.
If it is available in the future:
Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
Videoconferencing and webcam use will be appropriately supervised for the pupils age.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
Mobile phones will not be used during lessons or formal school time. Children bringing phones to school must hand them to their teacher as they enter school and collect them at the end of the day. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
The use by pupils of cameras in mobile phones is not allowed (See separate mobile phone guidance)

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to GDPR 2018.

Authorising internet access

All staff must read and sign the Staff Acceptable use of ICT before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor RBK can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling online-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

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

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Discussions may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

.

Introducing the online-safety policy to pupils

Online-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in online-safety has been be developed, based on the materials from CEOP

Online-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the online-safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Teachers of lower KS2 children will always use a child friendly safe search engine when accessing the web with pupils. However with the use of Google part of their ICT curriculum to raise awareness of some of the issues they may come across when using it at home.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the school online-safety policy in newsletters, the school brochure and on the school website.

The school will maintain a list of online-safety resources for parents/carers.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1 - Useful resources for teachers

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 2 - Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com