St Matthew's Church of England Primary School

Online Safety Policy

Introduction

At St Matthew's C of E School, we understand that online safety is not just about the safe use of the internet but all computing devices used within our school and wider community. We recognise the valuable contribution that the internet and digital computing devices can have on children's learning and can be a means of enhancing and engaging children in teaching and learning. We believe that the safe use of these technologies can be a beneficial teaching tool and aim to teach our children to use them responsibly, respectfully and independently.

Aims

We aim to use an embedded and cross-curricular approach to teach our children:

- To ensure their personal information always remains safe and to never provide it over a digital platform including but not limited to social media, email, blogs, gaming and websites.
- To understand that pop ups can lead to viruses or inappropriate content and that they should close them or block them if they occur. In school pop up blockers are always activated on iMacs, Macbooks, iPads and Chromebooks.
- That the internet should only be accessed in school with the permission of an adult and that if any inappropriate content appears that they should press the report button, minimise the screen and report the issue to a teacher immediately.
- That they should never arrange to meet someone in real life who they met in the online world unless arranged through a parent/carer.
- Children should not engage in communication online through websites or email without the presence or permission of a teacher.
- To communicate respectfully with others online and ensure that they do not say anything hurtful, racist or abusive to others. At St Matthew's we treat others, as we would like to be treated in both the real world and the digital world. Children are taught that emails must always be courteous and polite and teaching staff monitor our emailing system.
- Children know that they should not take photographs or upload any image without the person's permission.
- Children know that sites, games, videos and media have age ratings and why these ratings should be adhered to.
- Children are taught to recognise acceptable and unacceptable online behaviour and how these can affect other users.
- To ensure that their digital presence is positive and that appropriate filters, privacy settings and virus protections are needed.
- To take responsibility for their actions when interacting with digital technology and the reporting of ICT and online issues.
- To use only teacher permitted search engines and links while in school and in the presence of a member of teaching staff.
- That they should not download any software or app without adult permission.

Teaching and learning

At St Matthew's we acknowledge the internet is an integral part of 21st century living and the responsibility we have as educational practitioners to provide our children with an up to date safety curriculum which equips them with the skills they need in order to remain safe online. We understand that part of our duty is to provide children with quality internet access through a variety of devices; including tablets, laptops and desktops as well as the ability to apply the learning to mobiles and gaming devices, which they have in their homes.

The use of ICT and the internet is embedded throughout the curriculum to ensure pupils leave St Matthew's with a high level of digital literacy, which they will be able to apply to technological advancements in the future. Similarly, we use each of these opportunities to reinforce our online safety school ethos and key messages which are described above in the aims section.

As a school, we have developed an internet safety progression ladder (Appendix 1) to ensure our children are receiving an age-appropriate curriculum in every phase and year group. These statements have been created in accordance to the 2014 National Curriculum, April guidance for outstanding Online Safety Practice in schools (removed July 2014), surveys completed by our children surrounding their understanding of Online Safety, discussions with members of teaching and leadership staff. These have also been reviewed by governors, school council, parents and an Online Safety committee.

We use the C's- Content, Contact and Conduct- when discussing safety with our children. The use of this language ensures we are providing a well-rounded safety curriculum, which considers the three areas where children are likely to find dangers or issues.

We are committed at St Matthew's to safeguarding our children while providing an interactive, motivating and engaging curriculum which uses a wide range of resources including; DS consoles, Macbooks, Chrome books, iMacs and iPads.

Managing Internet access

School website

- The school website is edited by the Online Safety co-ordinator and DHT who ensures that all copyright laws and photo use permissions are abided to. An external company who has close links with school and is a member of the governing body manages the website.
- The only contact information detailed on the website is that of the school site and head teacher's email. All other staff's information should not be published.
- While the Online Safety coordinator takes control of the editing of the site, the head teacher takes overall responsibility for checking its accuracy and appropriateness.
- The website was designed and edited in line with DFE statutory requirements.
- The website contains an Online Safety page, which provides pupils, parents and the wider community with information on staying safe and line and the latest updates.

Email

- Pupils are only allowed to use school email addresses which are created as part of our learning platform and monitored by teaching staff.
- Pupils do not have individual email accounts but instead a class set of 30 email addresses have been created so that they can be used for the teaching of emails.
- Pupils are only allowed to email each other while a teacher is present and the class teacher, Online Safety co-coordinator and technician monitor the outgoing and incoming messages.
- When emailing school from home pupils are only allowed to use their class email address and not try to contact individual teachers directly.
- Only class email addresses are made available to parents and personal work email addresses remain private.
- Pupils are taught to use email respectfully and responsibly and are educated about the potential dangers of spam mail.

Learning platform

- We use Microsoft office as our online learning platform where we have a dedicated staff site.
- The passwords will only be accepted if they include numbers, letters and symbols and are required to be changed every 6 months.
- The staff site is only accessible to teaching staff.
- Staff are aware that they should not use the One Drive for storing any images of pupils or personal information about pupils or themselves.

Online resources for home learning

- Children have access to Mathletics at home. Each child has their own individual login and while they can play against other children in the school and world, they are not able to communicate with them. The head teacher who is also a safeguarding officer monitors this site.

Facebook

- The school operates a school Facebook page that is monitored and edited by the Online Safety Co-ordinator.
- Any follows remain anonymous and therefore safeguards our pupils and their families.
- Any content uploaded by school is subject to approval and our safeguarding policy in line with the consent documentation our parents sign.
- Any inappropriate comments or messages are to be deleted and reported by the assigned individual to Facebook, the Online Safety coordinator and the safeguarding team in school.

The internet in school

- The internet in school is filtered by our internet provider, Trust Net through Virgin Media and monitored by the Online Safety coordinator and ICT technician.
- Virus protection is updated annually and included on every device.
- If pupils come across any inappropriate content or have any issues they should click the report button, minimise the screen and tell an adult immediately. The website should be minimised instead of closed so that the member of staff can obtain the URL. The incident should then be reported to the safety coordinator and a safeguarding officer who will then investigate and inform Trust Net of the URL requiring blocking if investigations dictate that this is needed.
- Pupils are only allowed to use the internet when an adult is present and all computing devices have internet history so that we can track internet usage.
- You Tube is only allowed to be used by members of staff for teaching purposes and must never be accessed by children.
- Children sign and agree to an acceptable use policy which is approved by their parent/ carer.

Staff usage

- Staff may access You Tube but may only display a video which has been risk assessed prior to showing the pupils.
- Staff must not access social media sites on the school premises and should maintain the professional conduct while using the internet in line with the professional conduct strand of the teaching standards. Please see the school policy on social media usage for more information.
- Staff must use email respectfully and responsibility and understand that the technician has access to any email account should the need arise for an investigation into inappropriate use.
- Staff should model outstanding Online Safety awareness to pupils in their own use of the internet in lessons and should ensure that relevant Online Safety teaching points are embedded in their teaching.
- Staff must not access their personal email account (except for the learning platform) using the school internet system unless it can be proven that it is for the retrieval of an educational resource.
- Staff emails must not be opened in front of any child in school- with particular reference to the display on the IWB.

Introducing new technology in school

- All technology is risk assessed in terms of Online Safety for both children and staff and is potential impact upon learning.
- If a device or software is deemed to be a valuable resource in terms of teaching and learning then privacy setting, blocks and control measures are to be put into place before use by a child.
- New devices will also be given staff training to ensure up to date Online Safety knowledge and understanding and children will always participate in relevant Online Safety learning before using a new device.
- The introduction of new devices will be reviewed by the Online Safety coordinator, Computing leader, Head teacher, Safe guarding officer, ICT technician and the Online Safety committee.

Staff training

At St Matthew's we recognise that our staff need the most up to date information to be able to deliver an effective Online Safety curriculum. We also acknowledge our role in ensuring we provide training which helps to keep our staff safe online and help them to meet the professional conduct strand of the teaching standards.

- Staff will receive annual staff training in the delivery of Online Safety, developments in Online Safety and social media usage to be delivered by the Online Safety coordinator.
- Staff will complete and acceptable usage policy document.
- Staff will complete annually 1 x 30-minute online training course for Online Safety in school and 1 x 30-minute online training course for social media usage.
- Additional support will be provided where required and such training will always be provided to new members of staff before delivering the Online Safety curriculum.

Governors training

While governors play an essential role in the development and reviewing of the Online Safety policy, it is crucial that we provide appropriate training so that they are fully aware of their responsibility in ensuring whole school Online Safety. It is also essential that we provide governors with an understanding of how they themselves can remain safe online.

- Governors to receive an Online Safety update from the Online Safety coordinator annually.
- Ethos and values committee to meet to discuss Online Safety annually.
- 1 x 30-minute online training course annually for all governors that details their role and responsibility relating to Online Safety within school.

Parental involvement

With technological advancements and the now ease of access to the internet it is more important than ever to ensure we engage with parents surrounding Online Safety. As a school, we have two responsibilities: ensuring parents can support their child with Online Safety and the parents own online safety.

- We provide updates of Online Safety for both parents and their children through stands at the yearly 'meet the teacher' and termly parents evening.
- We engage parents through coffee mornings to discuss current issues and concerns.
- Online training is available for parents to engage with if they wish to sign up for the course.
- Parents are invited to whole school assemblies with an Online Safety focus.
- Parents are also invited to engage in inspire workshops, meetings with external agencies and to join the Online Safety committee.
- Parents are required to sign an acceptable use policy which details the school's requirements for their children.

Reaching out to the wider community

- Through the Online Safety committee, we aim to engage with members of external agencies who can work with our families to develop their Online Safety.
- By working as a cluster of schools we aim to share best practice between schools and reach more members of the community.

What is the Online Safety committee?

This is a committee that is made up of the Online Safety Co-ordinator, safeguarding officer, members of the governing body, members of the school council, members of teaching staff and parents. The committee meets to consider the effectiveness of internet safety in school, evaluate new technological advancements and consider the latest issues. This committee is important as the

technological world advances at and incredible rate and for us as a school to provide the best Online Safety possible for our children, parents, staff, governors and wider community we must ensure that we adapt to any advancement quickly.

Risk Assessment

St Matthew's will regularly audit the ICT/ computing provision to ensure its safety for the children's use. While precautions are in place and members of staff are continually vigilant, it is possible with the world scale of the internet for pupils to come across inappropriate material. In the unlikely event both pupils and staff will follow the reporting guidelines as detailed in this policy however the school and Sandwell LA do not accept liability for this material being accessed. This is detailed within the parental acceptable use policy.

Report an issue

Children should…
1. Use the report button
2. Minimise the screen
3. Tell an adult immediately

Staff should…
1. Retrieve as much information as possible including the URL
2. Staff should reassure the pupil
3. Report the incident as soon as possible to a safeguarding officer and the Online Safety coordinator.

Complaints

Any Online Safety complaint must be dealt with a member of the senior leadership team and required the head teacher. All issues surrounding safeguarding and child protection should be dealt with in line with the schools safeguarding policy and child protection act including the Child Protection Act and Data Protection Act.

General advice to teachers

- Ensure that children understand the importance of Online Safety.
- Refer to Online Safety in terms of content, contact and conduct
- Teaching should be appropriate to the age and ability of the child, and may vary across year groups and key stages but should be linked to the Internet Safety Progression Ladder.
- Embed Online Safety across the curriculum and do not limit it to the Computing lesson.
- Create a safe and welcoming ethos where pupils feel able to report issue.
- Always report issues following the guidance in this policy as quickly as possible after the incident.

Monitoring and review

We are aware of the need to monitor and update the school's Online Safety policy on a regular basis, so that we can take account improvements made in our practice. We will therefore review this policy yearly, or earlier if necessary. Ongoing informal reviews and discussions will take place throughout the year through the Online Safety committee.

Policy to be reviewed in Summer 2018

Appendix 1

Internet Safety Progression Ladder

Nursery	- Children know to tell an adult if they see something that upsets them. - Children know the need to close pop ups on the computer and apps. - Children know that they should only access the internet with adult permission and presence.
Reception	- Children know they should only take photos of people with their permission. - Children know what to do if they feel sad or uncomfortable when using a computer or tablet. - Children know that they should not tell a stranger their name, school or age. - Children know how to close pop ups on the computer and apps. - Children should pick technology appropriate to the task.
Year 1	- Children know to say 'kind words' to others through computing devices. - Children know that they should not talk to strangers on the internet. - Children can define the term personal information and know that they should keep it private. - Children know how to use the report button online. - Children know who to tell about an online incident at school and home.
Year 2	- Children are respectful online. - Children know how to select appropriate information in a search engine. - Children know what content is inappropriate for their age. - Children can define personal information and know how they can keep it private. - Understand the term contact and consider what contact is appropriate and inappropriate.

Year 3	- Children use email safely and respectfully and know that they should not disclose personal information through email. - Recognize unacceptable behavior online. - Children know how to report an issue online in school and at home. - Children can apply their understanding to tablets, desktops and laptops. - Children identify their responsibility to report issue.
Year 4	- Children are aware of 'junk' mail and potential risks within them. - Children recognize acceptable and unacceptable behavior online. - Children know how to protect information about themselves online. - Children can apply their understanding to tablets, desktops, laptops, game consoles and mobile phones. - Children identify the responsibility for their comments and interactions online.
Year 5	- Children are aware of pops up and how to control the pop up blocker. - Children know unacceptable behavior online can affect others. - Children know how to get things removed from social media websites. - Children can apply their understanding to any device. - Children identify their responsibility for the protection of their personal information.
Year 6	- Children understand how and why the school system is filtered, how they can filter at home and issues to be aware of when using unfiltered internet. - Children know how unacceptable behavior can affect their futures. - Children understand the term digital identity. - Children know how to have information about them removed from websites and google. - Children can identify ways in which they need to be responsible internet users.