ST MICHAEL'S C of E PRIMARY HIGHGATE

E-Safety during School Closure:
Guidance from School Governors

Concerned about a serious E-safety incident? Report to CEOP

(Child Exploitation and Online Protection)

https://www.ceop.police.uk/ceop-reporting/

What is E-Safety?

E-safety is the safe use of information systems and electronic communications, including the internet, mobile phones and games consoles. It is important that children and young people understand the benefits, risks and responsibilities of using information technology.

- e-safety concerns safeguarding children and young people in the digital world.

- e-safety emphasises learning to understand and use new technologies in a positive way.

- e-safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.

- e-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Using the Internet safely at home

Whilst many Internet Service Providers (ISPs) offer filtering systems to help you safeguard your child at home, it remains surprisingly easy for children to access inappropriate material including unsuitable texts, pictures and movies. Parents are advised to set the security levels within Internet browsers with this in mind. Locating the computer or tablet in a family area, not a bedroom, will enable you to supervise children as they use the internet. Do allow your child the opportunity to learn from the wide variety of material and games available on the Internet, but set some simple rules for keeping them safe and make sure

they understand the importance of these rules. See https://www.internetmatters.org/ for further guidance.

Rules for keeping your children safe:

To keep your child safe they should:

- Ask permission before using the Internet

- Only use websites recommended by the school or that you have chosen together, or allow them access via a child-friendly search engine only.

- Only email people they know (consider setting up an address book for them)

- Ask permission before opening an email sent by someone they don't know

- Do not use Internet chat rooms

- Do not use their real name when using games on the Internet (create a user name)

- Never give out a home address, phone or mobile number

- Never tell someone where they go to school

- Never arrange to meet someone they have 'met' on the Internet

- Only use a webcam with people they know

- Ask them to tell you immediately if they see anything they are unhappy with.

Using these rules

Go through the rules with your child and consider pinning them up near the computer. It is also a good idea to regularly check the Internet sites your child is visiting e.g. by clicking on History and Favourites. Please reassure your child that you want to keep them safe rather than take Internet access away from them.

Talking to your children about staying safe online

We regularly use our PSHE lessons to remind your children about the importance of staying safe online. You can use some of the resources at the links below to continue the conversation.

https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Gaming

Things you can do to keep your child safe online:

- check your parental controls on your PC to stop them accessing inappropriate material

- accessing games on a console or tablet? Here's how to set parental controls: Ask About Games

- have a conversation, discuss sites and apps together, talk about any concerns they may have

- talk about personal information and what not to share online

- is your child accessing social networks? Most of these have an age limit of 13+, check the content and age limits of what they are accessing here: NetAware

- Is your child playing computer games, check the age limit here: Netaware

Guidance on online group meet-ups:

1. Everyone at St Michael's C of E Primary School has the right to feel welcome, secure and happy in a positive environment. At our school there is a positive and respectful culture between all staff and learners creating an environment where bullying, peer-on-peer abuse or discrimination are not tolerated. We expect the same respectful culture to be maintained in all online meet-ups.

2. Unless you are inviting the whole class, do not publicise meetings on a whole class email/WhatsApp group as this will be upsetting for children not invited to the online meet-up. Email individual parents directly to make a time and date for a meeting.

3. Ask your child to agree to three golden rules for online meet-ups:

   - Have fun and enjoy seeing your friends
   - Don't discuss any child not in the meeting
   - No swearing or discriminatory language.

Class meet-ups via Zoom

With the increasingly widespread use of Zoom, there's been a rapid increase in "Zoom bombing" – uninvited participants dropping into Zoom meetings to share inappropriate or distracting audio, video, or images. To prevent this, please note the following safety tips for anyone using Zoom:

1. Avoid sharing your meeting link publicly (on social media or a public website). Share the link in a direct email and only to a parent you know personally.

2. Do not allow children to set up their own Zoom meetings without your initial oversight of invitees.

3. [Change your screen sharing settings](#) to "Host Only." This prevents anyone you don't know who has somehow accessed your meeting from sharing inappropriate content on their screen with the whole meeting.

4. Consider turning on the [Waiting Room feature](#). This will require the host to approve every participant before entry into the meeting. Keep in mind that if a participant is disconnected, you will need to re-approve them for entry, so this option requires keeping an eye on your Zoom notifications during the meeting.

5. Alternatively, consider locking your meeting (via the "Manage Participants" button in your Zoom tool tray) once all attendees are present. (Keep in mind that if a participant loses connection, they will not be able to re-enter unless you unlock the meeting).

6. For more information, see Zoom's blog post on the subject: [How to Keep the Party Crashers from Crashing your Zoom Event](#)

Online Private Tutoring

Please exercise the same level of caution as you would for having a tutor visit your home.

Check the Tutors credentials, references and that they are DBS checked and be mindful of the potential risks associated with 1:1 online contact

Acceptable Use Policies

All children have signed our ICT acceptable use policies, which can be found at the following links:

Key Stage 1:

https://stmichaelsn6.com/wp-content/uploads/2020/02/AUP-KS1-Pupil-Acceptable-Use-Policy-2020-ws.pdf

Key Stage 2:

https://stmichaelsn6.com/wp-content/uploads/2020/02/AUP-KS2-Pupil-Acceptable-Use-Policy-2019-ws.pdf

March 2020