St Michael's CE Primary School
Sydenham

Online Safety Policy

Agreed by the Governing Body on: *February 2017*

Signed (Chair): *Beryl Fielder*

Review Date: Spring 2020

Online Safety Policy

This policy applies to all members of St Michael's CE Primary School, including staff, pupils, volunteers, parents / carers, visitors and community users who have access to and are users of school ICT systems, both inside and outside the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's published Behaviour Policy and Disciplinary Code of Practice.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

Also see:

- Social media and mobile phone policy
- Home School Agreement
- Staff Handbook/Code of Conduct
- Data protection policy
- Data security policy

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online incidents and monitoring reports. The Governor assigned for safeguarding will also act as Online Safety Governor. The Online Safety Governor will regularly monitor the online incidents and report to relevant governors as appropriate

Headteacher and Online Safety Leader (School Business Manager)

Has a duty of care for ensuring the safety (including online) of members of the school community and will:

- be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff,
- ensure staff receive suitable training to enable them to carry out their online roles and to train other colleagues, as relevant,
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- receive reports of online incidents and create a log of incidents to inform future online developments.

- take day to day responsibility for online issues and has a leading role in establishing and reviewing the school online policies / documents, in liaison with the headteacher
- report regularly to Governors.

The School Business Manager in liaison with the IT support company:

is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets required online technical requirements and any Local Authority / other relevant body / Online Policy / guidance that may apply.
- users may only access the networks and devices through properly enforced password protections.
- the Internet Service Provider (ISP) has a suitable filtering policy for use in schools and that any amendments to the filtering arrangements can only be requested by the headteacher or a previously authorised nominated contact.
- they keep up to date with online technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- the use of the network / internet / Virtual Learning Environment (if used) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher.
- passwords are not shared and in the event of a password being compromised that the user's password is immediately reset.

Teaching, Support Staff and Volunteers

are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current online policy and practices,
- they have read, understood and adhere to the guideline as stated in the staff handbook
- they report any suspected misuse or problem to the Headteacher for investigation/action/ sanction,
- all digital communications with students, pupils, parents and carers should be on a professional level and only carried out using official school systems,
- online issues are embedded in all aspects of the curriculum and other activities
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- ensure pupils understand and follow the online and acceptable use policies
- ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Child Protection / Safeguarding Designated Person

should be trained in online issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the 'Think Before you Click' document as well as the Social Media Policy (if appropriate, e.g. making posts on social media websites),
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying,
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the *school's* Online Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and/or mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online campaigns and literature. Parents and carers are expected to sign the 'Think before you Click' documents. Parents and carers will also be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog
- their children's personal devices in the school (where this is allowed)

Parents are not to post or publish discriminatory, defamatory, malicious or potential misleading information or comments regarding the school, its pupils, staff or governors on any form of social media (e.g. facebook, twitter, etc). This could potentially lead to a banning order.

Educating our pupils and parents

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Online safety should be provided as part of computing/circle time/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should be helped to understand the need for the 'Think before you Click' agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is planned, it is best practice that pupils should be guided to sites previously checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the request.

Many parents and carers have only a limited understanding of online risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, website
- Parents / Carers workshops / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Use of digital and video images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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 e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images.

Parents and carers are prohibited from recording conversations with members of the staff. This is due to Safeguarding and Data Protection issues that may arise from inappropriate use of the content recorded.

Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital/video images that students/pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without permission.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association wiith photographs.

Written permission is obtained from parents or carers in the home school agreement to seek permission to publish photographs on the school website.

School Actions & Sanctions

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of websites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and/or disciplinary procedures.

	Staff and adults				Children			
Communication Technologies A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school		✓						✓
Use of mobile phones in lessons	✓				✓			
Use of mobile phones in social time		✓			✓			
Taking photos on personal mobile phones / cameras	✓				✓			
Use of other (not personal) mobile devices eg tablets, gaming devices			✓					✓
Use of personal email addresses in school, or on school network			✓		✓			
Use of school email for personal emails	✓				✓			
Use of messaging apps	?		✓		✓			
Use of social media	?		✓		✓			
Use of blogs (the school blogsite)			✓					✓

Think before you click: Responsible Internet Use Agreement

Please read the following and complete this form if you are in agreement. If there are any sections which you do not agree with please indicate this by putting a line through the relevant section.

PUPIL _____ CLASS _____

THINK BEFORE YOU CLICK

S

A

F

E

- I will ask permission before entering any website, unless my teacher has already approved that site;
- On a network, I will use only my own login and password, which I will keep secret;
- I will not look at or delete other people's files;
- I will not bring CD ROMs or USB keys into school without permission;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone;
- I will not use internet chat;
- If I see anything I am unhappy with or I receive messages I do not like, I will tell my teacher immediately;
- I know that the school may check my computer files and may monitor the internet sites I visit;
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers;
- I understand that if I use a computer or phone at home, I need to use it in a responsible manner or I may face consequences at school.

Pupil's Agreement

I have read and understood "Think before you click". I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: _____ Date: _____

Parents'/Carers' Consent

Internet Access

I have read and understood "Think before you click" and will talk to my child about it. I give permission for my child to access the internet.

I give permission for my child to use electronic mail and their learning platform account. I understand that the school will take all responsible precautions to ensure pupils cannot access inappropriate materials.

I understand the school cannot be held responsible for the nature or content of materials accessed through the internet.

Web Publication of Work

I agree that, if selected, my son/daughter's work may be published on the school website.

Publication/Use of Photographs

I agree that photographs/images of my son/daughter may be published on the understanding that full names will not be used.

Parent_____ Pupil_____ Date_____

E-LEARNING CODE OF CONDUCT-YOUNG USERS

You should:


Always follow the instructions of your teacher.


Keep your username and password secret.


Always be nice and polite when you send messages to other users.


Always tell your teacher if you see, hear or read anything which makes you feel uncomfortable while using the computer.

You should not:


Send anyone a message which is not nice.


Use bad language in a message.


Use any other person's work or email.


Tell a stranger any of the following:

- Your name
- Your home address
- Your telephone numbers
- Any other personal information about yourself or any of your friends.

When you are finished using a computer you should always close it down properly following your teacher's instructions.