St John with St Mark C E Primary School

E-SAFETY POLICY 2017

Development

This e-safety policy has been developed by the *E-safety/Computing Coordinator*, in consultation with:

- *The Headteacher*
- *A Parent school governor (governor for health & safety)*
- *The whole staff team **
- *The school council ***

**All teachers and teaching assistants were presented with the details of the policy in draft form, with opportunity given for feedback and suggestions.*

***The school council were also consulted as part of the preparation of the policy. The minutes for their meeting are attached to the back of this policy.*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body	*7 / 11 / 2017*
The implementation of this e-safety policy will be monitored by the:	*E-safety Coordinator* *Senior Leadership Team*
Monitoring will take place at regular intervals:	*Monitored annually in April*
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually in April*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*April 2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager* *LA Safeguarding Officer* *Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
    - groups of pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator: **(Simon Sadler)**

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager:

Technical Staff (PCEdutech) are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher, Senior Leadership Team or E-Safety Coordinator
- all digital communications with pupils / parents / carers are on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils are guided to websites you have checked for suitability. For internet searches, pupils are to use http://www.kidzsearch.com/

Child Protection / Safeguarding Designated Person

Should be trained in e-safety 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 Pupil Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, the school website and E-safety assemblies.

Policy Statements

Education –pupils

It is important that pupils are taught how to use digital technology in a responsible way. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Key e-safety messages will be summarised with the slogan: *"Zip it – Block it – Flag it"*

These key e-safety messages should be reinforced across the curriculum. This will happen in the following ways:

- The computing curriculum contains an E-communication unit. This covers key e-safety messages that are built upon each year. These key messages are to be referred to in other units too.
- Key e-safety messages will be reinforced in termly e-safety assemblies for the whole school.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement. They should be encouraged to follow these rules both in and out of school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role how their children use technology and internet. Parents may underestimate how often children 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, school website*
- *Parents evenings and September year ahead meetings*
- *High profile events e.g Safer Internet Day*
- *Invitation to attend termly E-safety assemblies*
- *Invitation to attend staff training sessions*

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. Staff will be trained on an annual basis.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions,

This will be offered in the following ways:

- Participation in staff training sessions
- Attendance at termly E-safety assemblies

Use of digital and video images

Alongside the many positives, there are also risks associated with publishing digital images and videos on the internet. Staff, parents and children need to be aware of these risks. The school will seek to reduce the likelihood of the potential for harm in the following ways:

- When using digital images, staff should inform 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 pupils in the digital / video images.

- Staff and volunteers 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 pupils are appropriately dressed and 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 their 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 with photographs.

- Parents/Carers will have opportunity to sign to request that no image or video of their child is used on the school website or blogs

Communications

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:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	√							X
Taking photos on personal phones / cameras / tablets				X				X
Use of other mobile devices eg tablets, gaming devices		√						X
Use of personal email addresses in school, or on school network	√							X
Use of chat rooms / instant messaging				X				X
Use of social media				X				X
Use of blogs (other than the school blog)		√					√	

Pupils and mobile phones

In normal circumstances, pupils are not allowed to bring a mobile phone into school. However, it is recognised that under some unusual circumstances there is a need for children to bring a mobile phone to school. If this is the case, the parent must speak to a member of the leadership team to request permission and explain the situation. The mobile phone would then be placed in the care of a member of staff during the school day, ready to be taken home at the end of the day.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

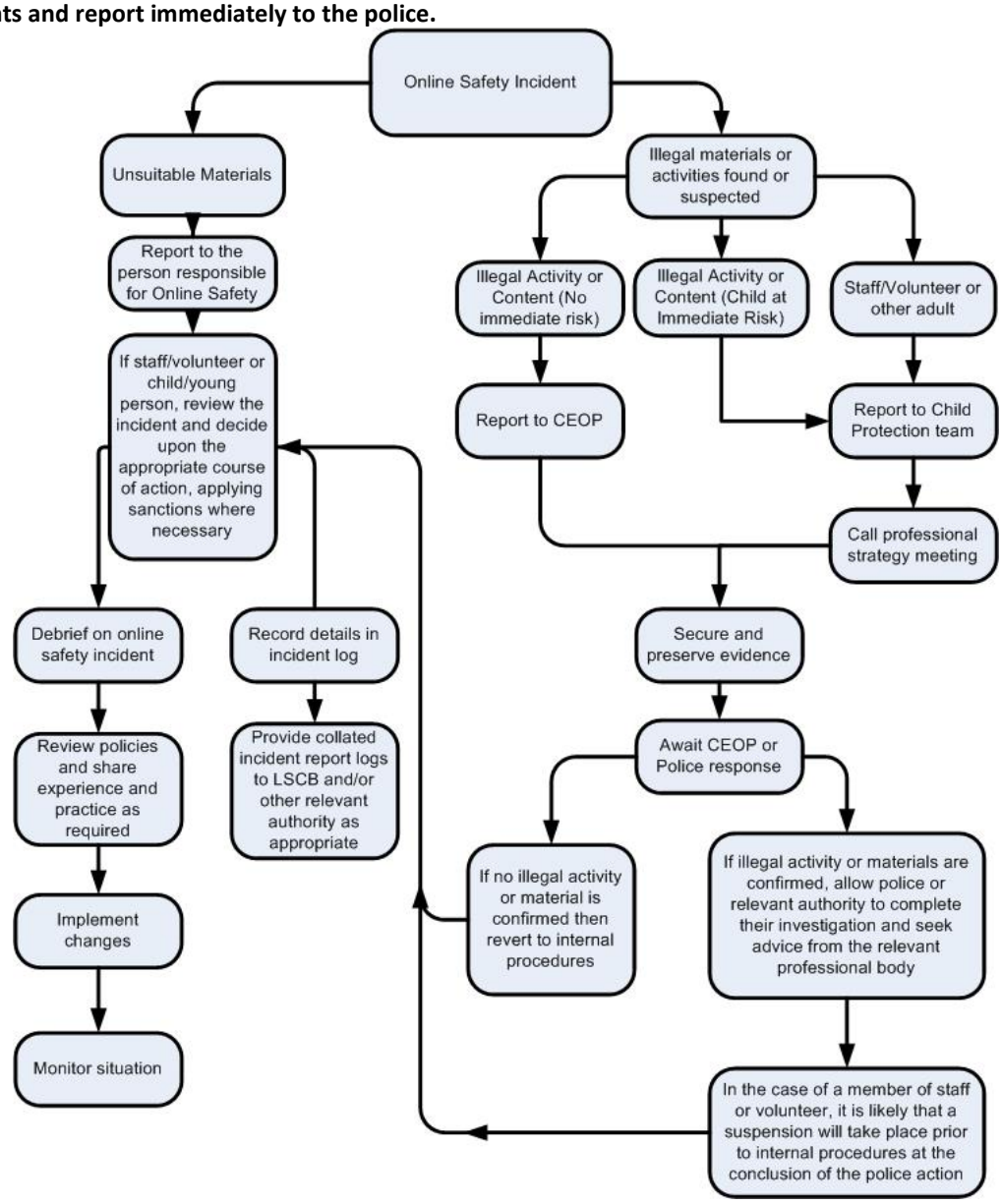
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendices

* KS2 Acceptable Use Policy

* KS1 Acceptable Use Policy

* Staff Acceptable Use Policy

* E-safety Incident Logging Records

* School Council Consultation notes

Pupil Acceptable Use Agreement - KS2

This Acceptable Use Policy is to make sure that when you use technology and the internet:

- you are kept safe
- school equipment is kept safe

Please make sure you read and understand the following statements.

- I will only use ICT in school for school purposes
- I will not use my own email address in school
- I will only open email attachments from people I know or who my teacher has approved
- I will not tell other people my ICT passwords
- I will not take a photo of someone if I haven't asked them first
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will tell my teacher or Mr Sadler if:
    - I see or receive something unpleasant or nasty online
    - Someone is bullying me online
    - A stranger is asking about my personal information online
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will look after all ICT equipment, including anything I take home (a kindle)
- I will only download an app or kindle book with permission from my teacher
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

Pupil Acceptable Use Agreement - KS2

User Signatures

Class _____ Date _____

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Pupil Acceptable Use Agreement - KS1

This Acceptable Use Policy is to make sure that when you use technology and the internet:

- you are kept safe
- school equipment is kept safe

Here are the rules you need to know and say yes to:

- I will look after the computers and iPads I use
- I will tell a grown up if something pops up on the screen
- I will only talk to people I know on a computer
- I will not take a photo of someone if they don't want me to
- I will not give my personal information to people I don't know online
- I will tell a grown up if I see something that upsets me

Pupil Acceptable Use Agreement - KS1

User Signatures

Class _____ Date _____

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Staff Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their **professional responsibilities** when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher or Computing Coordinator.

- I will only use the schools email/internet and any related technologies for professional purposes of for uses deemed "reasonable" by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will ensure that personal data (such as data held on Integris) is kept secure and is used appropriately whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body
- I will not install any hardware/software/apps without permission of the Computing Coordinator/ Headteacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or member of staff. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school , will not bring my professional role into disrepute
- I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not upload content that is inappropriate, offensive or even illegal to my online spaces at school or post material that could damage the reputations or the reputations of others or breach intellectual property rights
- I am aware that posting inappropriate comments to the profiles of others can result in bullying or humiliation for the person or potential charges of libel for the perpetrator

Staff Acceptable Use Agreement

Staff Signatures

Date _____

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Reporting Log

Reporting Log Group									
Date									
Time									
Incident									
Action taken	What?								
	By whom?								
Incident Reported by									
Signature									

SCHOOL COUNCIL
E-SAFETY CONSULTATION

Date:
15.9.2017

Council Members present:
Amelia Foster, Moeez Naeem, Maisey Mills, Thomas, Haleema Zubair, Jake O'Donnell, Monisa Batool, Aman Ahmed, Jake Singh, Hira, Ayesha Q, Ayesha I.

1. Why could the internet sometimes be unsafe for children?

* Social media – fake identity/cyber bullying
* Personal information given out
* Gaming sites e.g. Xbox – information given and feeling threatened/bullied
* YouTube – voice recognition or misspelt words can lead to inappropriate words or images
* Playing inappropriate or age-restricted games
* Misleading games/apps – they look appropriate but are not suitable

2. What do you think the school should do to help keep you safe on the internet?

* Information given to families about how to keep safe on the internet. Also, give a list of websites suitable for children's learning
* Warning letter home to parents about age restrictions on social networking sites
* Inform parents about 'safesearch' for images

3. Who would you go to in school if you felt unsafe on the internet?

* Tell a friend first and then both go and tell any teacher
* Tell my friends – telling a teacher would make me feel uncomfortable