ST MICHAEL & ALL ANGELS C OF E PRIMARY SCHOOL

E-safety Policy

Date Approved	**29.11.16**
Date for Review* *(*subject to any relevant changes in legislation or other appropriate guidelines)*	**November 2019**
Policy Last Revised	**November 2016** ***Appendix 1 added 22.6.18*** ***Appendix 2 added 21.8.18***
Author	Head Teacher
Delegated Responsibility	Health & Safety Committee

Approved by:	M Field
	Chair of Committee
Date received by FGB	29.11.16

1. Introduction

1.1 St Michael & All Angels CE Primary School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at St Michael's want to ensure that new technologies are used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

1.3 We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give disabled pupils increased access to the curriculum to enhance their learning.

1.4 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated senior person for the implementation of the School's e-Safety policy is Mr Neil Bardsley, Head Teacher.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 St Michael's will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;

- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;
- close supervision of pupils when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 St Michael's recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is Primary World who provide a managed (not 'locked down') network system. We fully support and will continue to work with Primary World to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures .

3.1.3 We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

4.1.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 St Michael's expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

[1] For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

Users are not allowed to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by the Head Teacher, so that the action can be justified, if queries are raised later.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

4.1.5 In addition, users are not allowed to:

- Use Primary World or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves Primary World or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of Primary World or member Local Authorities or adversely impact on the image of Primary World;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Primary World, or to Primary World itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:

- financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via Primary World.
- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via the Primary World network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the Primary World network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after Primary World has requested that use cease because it is causing disruption to the correct functioning of Primary World ;
    - other misuse of the Primary World network, such as introduction of viruses.
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.1.6 If Primary World become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

4.2.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately.

4.2.2 The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB[2] Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 St Michael's recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

5.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

5.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.
- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures .

[2] Chapter 9 of the LSCB Procedures
[3] Chapters 5, 9, 12 and 13 of the LSCB Procedures

6. Standards and Inspection

St Michael's recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 The school has a right to monitor staff use of the internet and electronic mail at any time deemed necessary.

6.1.2 We will monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 We will support pupils and staff as necessary in the event of a policy breach.

6.2.2 Where there is inappropriate or illegal use of technologies, the following sanctions will be applied:

- *Child / Young Person*
    - The child/young person will be disciplined according to the behaviour policy of the school.
    - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- *Adult (Staff and Volunteers)*
    - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
    - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to Mr Bardsley so this can be taken into account for monitoring purposes.

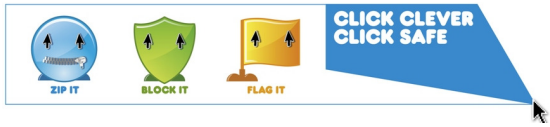
7. Working in Partnership with Parents and Carers

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We also appreciate that there may be some parents who are concerned about the use of the technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 Related aspects of the school's E-safety policy include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention.



E-safety Checklist for Schools

Policies, practice and monitoring	Yes	No	Action
Does the school have an e-safety policy in place?			
Are there 'Acceptable Use Policies' for both pupils and adults?			
Is cyber bullying addressed in the school's anti-bullying policy?			
Are there effective sanctions in place for breaching the policy?			
Has the school appointed an e-safety co-ordinator?			
Is e-safety provision rigorously and regularly reviewed?			
Does the school keep a log of e-safety incidents and alter provision if necessary?			
Has an evaluative comment on e-safety been included in the SEF?			
Infrastructure	**Yes**	**No**	**Action**
Is the school network safe and secure?			
Does the school use an accredited internet service provider? *Eg embc*			
Does the school use internet filtering/monitoring?			
If there are changes made to the internet filtering setup are these authorised by a senior manager?			

Learners	Yes	No	Action
Do learners understand what safe and responsible online behaviour means and do they use it?			
Is e-safety education a regular part of the curriculum?			
Do learners know and understand the UKCCIS digital code – 			
Do learners know how to report e-safety concerns they may have? *Eg CEOP Report Abuse button, reporting to an adult in school*			
Staff	**Yes**	**No**	**Action**
Do teaching staff understand e-safety issues and risks?			
Have they received training which is regularly updated?			
Do staff know who to report to with an issue of concern regarding e-safety?			
Do they keep data safe and secure? Eg encrypted personal assessment data, use of password protection			
Do they take measures to protect themselves online? *Eg keep personal information private, use secure passwords*			
Do they conduct themselves professionally online? *Eg social networking sites, blogs*			
Parents / Governors	**Yes**	**No**	**Action**
Do governors have a general understanding of the issues and risks associated with e-safety?			
Does the school keep parents aware of e-safety issues through eg newsletters, leaflets, open assemblies, updates etc?			
Has the school held an e-safety Parent Awareness Session?			

Source acknowledgement: "Safeguarding children online – How e-safe are your school and your learners?" BECTA

E-safety Log of Incidents

This form should be used to keep a log of the type of e-safety incidents that occur over a school term and to record the response in each case. The log can be used to highlight any particular trends and to inform e-safety management decision-making. Place a tick in the appropriate box on the grid for each incident reported.

Year _____ **Term** _____ **Room** _____	Referred to class teacher	Referred to Line Manager	Referred to Head Teacher	Referred to Police	Referred to technical staff for action eg filtering	Informed parents	Warning given	Sanction / disciplinary action
Deliberately accessing illegal material								
Unauthorised use of non-educational sites								
Unauthorised use of mobile phone / digital camera / other handheld device								
Unauthorised use of social networking / instant messaging / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing passwords								
Attempting to access the school network using another student's account								
Attempting to access the school network using the account of a member of staff								
Corrupting or destroying the data of other users								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								

Source acknowledgment: SWGfL School E-safety Policy

E-safety Incident Record

Use this form to record the details of serious e-safety incidents and the action taken. Hand to _____ (e-safety co-ordinator) for monitoring purposes.

E-safety incident					
Name of staff member discovering		**Date**:		**Time**:	
Name of pupils / staff involved					
Nature of incident (tick box)	Failing to report accidental access to inappropriate material	Intentional access to inappropriate material	Cyber Bullying	Grooming	Other
Details					
When incident occurred (tick)	During a lesson	Outside lesson time	Outside school		
Is police involvement needed? (Yes if…)	Grooming / Indecent images of children	Criminally obscene material	Criminally racist or discriminatory	Violent / bomb making	Other criminal conduct
Signed by Head Teacher		Date:	Time:		
STAFF **Action taken eg HR contact, Chair of Governors, disciplinary action, police**					
PUPIL **Action taken eg Contact parents, sanction applied, police**					

Cyberbullying - Advice for schools:
Regulating off-site behaviour and applying sanctions in response to Cyberbullying

In response to queries from schools, please see below a summary of government guidance.

Cyberbullying can be defined as:
'The use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else'
(DCSF Safe to Learn)

It is very important for schools to take Cyberbullying seriously. Although Cyberbullying is not a specific criminal offence in UK law, there are criminal laws that can apply.

Taking a whole school approach to preventing Cyberbullying is essential. Education and discussion around responsible use and e-safety is key to helping young people to act responsibly and deal confidently with any problems that may arise whether in or out of school.
Schools should ensure that anti-bullying policies and behaviour policies are reviewed and updated to include Cyberbullying; also consider the impact on a range of other policies – staff development, ICT support, acceptable use policies and e-learning strategies.

Schools should publicise not only the support available for students and how to report bullying, in addition, any rules and sanctions relating to the misuse of technology must be well publicised with both students and parents.

Bullying is never acceptable and the school community has a duty to protect all its members and provide a safe, healthy environment.

The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to Cyberbullying.

Head teachers have the power 'to such extent as is reasonable' to regulate the conduct of pupils when they are off-site.

So what does this mean for schools in practical terms?
Government guidance states 'an effective policy on school discipline and pupil behaviour should also set expectations for positive behaviour off the school site'

Further:

'Schools must act reasonably both in relation to expectations of pupil behaviour, and in relation to any measures determined for regulating behaviour by pupils, when off the school site and not under the lawful control or charge of a school staff member. **Ultimately only a court of law could**

decide what was reasonable in a particular case, but schools should decide what to take into account in deciding whether a rule or sanction is reasonable'

When determining the appropriate response and proportionate sanctions, it is important to consider the ways in which Cyberbullying incidents might differ in impact to other forms of bullying; the public nature of posted material, the extent of the humiliation and the difficulty in controlling copies of the material and therefore gaining closure over the event.

Guidance states that a school could sensibly take account of:
'The extent to which the behaviour in question would have repercussions for the orderly running of the school, and /or might pose a threat to another pupil or member of staff (e.g. bullying another pupil or insulting a member of staff)'

School Discipline and Pupil Behaviour Policies guidance states:

'New media (such as mobile phones, internet sites and chat rooms) can be exploited by pupils in order to bully or embarrass fellow pupils or members of staff. **Schools should make clear in their behaviour policy that the use of defamatory or intimidating messages and images inside or outside of school will not be tolerated, and that disciplinary sanctions will be applied to perpetrators…..**
……Head teachers should adopt firm measures against abuse or intimidation of staff. This includes unacceptable conduct by pupils when not on the school site, and when not under the lawful control or charge of a member of staff of the school'

Appropriate disciplinary sanctions should be applied when the pupil is next in school.

For more detailed information please refer to:

School Discipline and Pupil Behaviour Policies guidance:
www.teachernet.gov.uk/wholeschool/behaviour/schooldisciplinepupilbehaviorpolicies/

DCSF Safe to Learn: Embedding anti-bullying work in schools – Cyberbullying
DCSF Cyberbullying: Supporting School Staff
The DCSF Suite of guidance is available on our website
www.beyondbullying.com

For further advice please contact:

Sue Bosley
Anti-Bullying Strategy Manager
Sue.bosley@leics.gov.uk
Tel: 0116 3055114

Appendix 1

E-safety Scheme of Work

EYFS	http://www.kidsmart.org.uk/teachers/ks1/sources/index.htm
Year 1	Hector's World – Personal Information (Episodes 1-3)
Year 2	Hector's World – Personal information –(Episodes 4-6) Face to Face v emailed communication
Year 3	http://www.thinkuknow.co.uk/ **8_10/cybercafe/** Cyber-Cafe-Base/ Privacy and passwords
Year 4	http://www.thinkuknow.co.uk/ **8_10/cybercafe/** Cyber-Cafe-Base/ Sensitive Information (Cyber people)
Year 5	http://www.thinkuknow.co.uk/ **8_10/cybercafe/**

	Cyber-Cafe-Base/ Images and cyberbullying
Year 6	How to keep our identity private Mobile phones

Appendix 2

ST MICHAEL & ALL ANGELS C OF E PRIMARY SCHOOL

Rules for Responsible Internet Use

These rules will help keep us safe and help us be fair to others.

Using the computers/I-pads:

- **I will only access the computer system with the permission of my class teacher;**
- **I will not access other people's files;**
- **I will not bring in memory sticks, CDs or DVDs from outside school and try to use them on the school computers.**

Using the internet:

- **I will ask permission from a teacher before using the internet;**
- **I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;**
- **I understand that the school may check my computer files and may monitor the internet sites I visit;**
- **I will not complete and send forms without permission from my teacher;**
- **I will not give my full name, my home address or telephone number when completing forms.**

Using e-mail:

- **I will ask permission from a teacher before checking the e-mail;**
- **I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;**
- **I understand that e-mail messages I receive or send may be read by others;**
- **The messages I send will be polite and responsible;**
- **I will only e-mail people I know, or my teacher has approved;**
- **I will only send an e-mail when it has been checked/approved by a teacher;**
- **I will not give my full name, my home address or telephone number;**
- **I will not use e-mail to arrange to meet someone outside school hours.**