E-SAFETY POLICY

March 2021

St Michael's Primary School

E-Safety Policy

Rights Respecting Schools

St Michael's Primary School is a Rights Respecting School. All pupils, staff and visitors have the right to be healthy, safe, educated, listened to and treated fairly. These principles are at the heart our school ethos and our policies and practices support these rights. We are committed to equal rights, mutual respect and shared responsibility.

In this Policy we specifically recognise the following articles from the UN convention on the Rights of the Child:

Article 3 (Best interests of the child): The best interests of children must be the primary concern in making decisions that may affect them. All adults should do what is best for children. When adults make decisions, they should think about how their decisions will affect children. This particularly applies to budget, policy and law makers.

Article 13 (Freedom of expression): Children have the right to get and share information, as long as the information is not damaging to them or others. In exercising the right to freedom of expression, children have the responsibility to also respect the rights, freedoms and reputations of others. The freedom of expression includes the right to share information in any way they choose, including by talking, drawing or writing.

Article 16 (Right to privacy): Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Article 17 (Access to information; mass media): Children have the right to get information that is important to their health and well-being. Governments should encourage mass media – radio, television, newspapers and Internet content sources – to provide information that children can understand and to not promote materials that could harm children. Mass media should particularly be encouraged to supply information in languages that minority and indigenous children can understand. Children should also have access to children's books.

***Article 28*:** Every child has the right to an education.

Rationale/Vision

Boards of Governors have a duty to:

- **Safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries N. I. Order 2003).**
- **Determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries N.I. Order 2003).**

In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital

technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

What is E-Safety?

E-Safety is short for electronic safety. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions.

E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. E-Safety in the school context is:

- **Concerned with safeguarding children and young people in the digital world; emphasises learning to understand and use technologies in a positive way;**
- **Less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;**
- **Concerned with supporting pupils to develop safer online behaviours both in and out of school;**
- **Concerned with helping pupils recognise unsafe situations and how to respond appropriately.**

The rapidly changing nature of the Internet and new technologies means that E-Safety is an ever growing and changing area of interest and concern.

This E-Safety policy reflects this by keeping abreast of the changes taking place. The school has a duty of care to enable pupils to use on-line systems safely. This E-Safety policy contains aspects in relation to use of the internet, use of mobile phones and use of digital/photographic images of children.

It is largely based on DENI Circular 2007/1 *"Acceptable Use of the Internet and Digital Technologies in Schools"*, DENI Circular 2011/22 *"Internet Safety"*, DENI Circular 2013/25 *"eSafety Guidance"* and DENI Circular 2016/27 "Online Safety" and Safeguarding Board for Northern Ireland (SBNI Report - January 2014) and The General Data Protection Regulation (GDPR) (EU) 2016/679

https://www.education-ni.gov.uk/publications/circular-201627-online-safety

It should also be read in conjunction with the School's Safeguarding Policies.

ICT is a compulsory element of the NI Curriculum and schools must ensure acquisition and development by pupils of these skills. The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction.

Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The DENI circular 2007/01 states that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in St Michael's Primary School.

We aim to develop systems of safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies.

The policy has been drawn up by the staff of the school under the leadership of the Principal and ICT Co-ordinator. It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested.

The policy and its implementation will be reviewed annually.

Internet Services Connectivity and Filtering

Internet access is filtered for all users. The school has two internet systems in its infrastructure. Illegal content is filtered by both providers.

C2k

Classroom 2000 (C2k) is the project responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Some of these safety services include:

- ***Providing all users with a unique user names and passwords***
- ***Tracking and recording all online activity using the unique user names and passwords***
- ***Scanning all C2k email and attachments for inappropriate content and viruses***
- ***Filters access to web sites***
- ***Providing appropriate curriculum software.***

'Securus' forms part of the e-Safety suite of tools available to schools via the C2k network to safeguard children in their use of information systems and electronic communications. It monitors the screen display and keystrokes of students on C2K MANAGED MACHINES ONLY and triggers a capture if the content is listed in the database of inappropriate words and phrases.

Should the school decide to access online services through service providers' other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

Classnet

The school installed its own BT Internet line to enable the large number of iPads in the school to access on-line internet services. The Classnet connectivity and filtering system has built in firewalls, filtering and software monitoring mechanisms. The school will take appropriate measures to safeguard this non C2k equipment against security breaches.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Code of Safe Practice for pupils and staff containing E-Safety Rules which makes explicit to all users what is safe and acceptable and what is not. These will be discussed with pupils at the beginning of each school year as part of their class charter. (See Appendices)

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) is subject to the same requirements as technology provided by the school.

The ICT Co-ordinator and the Senior Management Team will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

A parental/carer consent for pupil is gained through our "General Schools Policy" accompanied by the "Rules of Responsible Internet Use" and "Photograph Permission". This is signed by parents/carers when the pupil first arrives to St Michael's in Year 1 and for any child who joins the school throughout the school year. This consent must be obtained before the pupil accesses the internet.

In addition, the following key measures have been adopted by St Michael's Primary School to ensure our pupils do not access any inappropriate material:

The school's E-Safety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and E-Safety guidelines are displayed prominently throughout the school;

- ***E-Safety guidelines are displayed prominently throughout the school;***
- ***Our Code of Practice is reviewed each school year and signed by pupils/parents;***
- ***Pupils using the Internet will normally be working in highly-visible areas of the school;***
- ***All online activity is for appropriate educational purposes and is supervised, where possible;***
- ***Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group;***
- ***Pupils in Years 4 -7 are educated in the safe and effective use of the Internet, through a number of selected websites;***
- ***Pupils will not access social networking sites in school.***

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours.

Pupil Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Positive Behaviour Policy. Minor incidents will be dealt with by the principal and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's Child Protection Policy.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff: (An example of an ICT Safe Code of Practice Agreement which staff can be asked to sign when taking up post is attached for information)

- ***Pupils accessing the Internet should be supervised by an adult at all times.***
- ***Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.***
- ***All pupils using the Internet have written permission from their parents.***
- ***Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator.***
- ***In the interests of system security staff passwords should only be shared with the network manager.***
- ***Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.***
- ***Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.***
- ***Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work.***
- ***School systems may not be used for unauthorised commercial transactions.***

Internet Safety Awareness

In St Michael's Primary School, we believe that, alongside having a written E-Safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication both inside and outside the school. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils. E-Safety awareness will be fully embedded in all aspects of the curriculum.

Internet Safety Awareness for Pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 2 pupils are made aware and discuss Internet Safety through structured lessons using a range of online resources e.g. ThinkUKnow, Child Exploitation and Online Protection (CEOP), KidSMART. The assigned KS2 Digital Leaders will promote the importance of Internet Safety throughout the school – especially in February – Safer Internet Day.

Internet Safety Awareness for Staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

The Child Exploitation and Online Protection Centre **(CEOP)** run regular one-day courses for teachers in Northern Ireland. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the Thinkuknow website.

Internet Safety Awareness for Parents

The Internet Safety Policy and Code of safe Practice for pupils is available on our school App and Website. Additional advice for parents with internet access at home also accompanies this letter or Internet safety leaflets for parents and carers also are sent home annually. The school organises a biannual talk on Internet Safety, usually delivered by PSNI for parents and the community.

Health and Safety

In St Michael's PS we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources in classrooms which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, IWB and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc. We are also mindful of certain medical conditions which may be affected by use of such equipment e.g. photosensitive epilepsy.

Risk Assessments

Life in the 21st century presents dangers including violence, racism and exploitation from which pupils need to be protected. The school to the best of its knowledge has considered all new technologies wisely to ensure that it is fully aware of and can mitigate against the potential risks involved with their use. In doing so, pupils are informed of what to do if they come across inappropriate material on line.

Use of Mobile Phones

Most modern mobile phones have internet connectivity.

Digital and Video Images

Parental permission is gained when publishing images and videos on the website, Twitter, Seesaw or otherpublications. Images are stored on a centralised area on the school network or individual class iPad's, Kindles and Chromebooks.

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available at: The Health Protection Agency website.

Cloud Storage

Data and information is stored on the Cloud, meaning it can be accessed from any location removing the need to carry data and files on memory pens and portable devices**.**

SeeSaw and Google Classroom/Meet Online Learning Forums

SeeSaw (P1-P4) and Google Classroom (P5-P7) online platforms are in use for homework and online digital communication. A Code of Conduct for Google Classroom and Google Meet is discussed with all children at the start of each academic year. (Appendix 2 and 3) SeeSaw terms of service can be viewed here : https://web.seesaw.me/terms-of-service

Web Site and School Twitter Account

The school Twitter account and web site http://www.stmichaelsps.com/ promotes and provides up to date information about the school as well as is used to celebrate pupils' achievements. Editorialguidance will ensure that these sites reflect the school's ethos that information is accurate and well-presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's Web site can be accessedby anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- ***The point of contact on the Web site should be the school address, school email and telephone number. Staff or pupils' details will not be published.***
- ***Web site photographs that include pupils will be selected carefully.***
- ***Consent from parents or carers will be obtained before photographs of pupils are published on the school Web site***
- ***Pupils' full names will not be used anywhere on the Web site or Twitter, particularly inassociation with photographs.***
- ***The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.***
- ***The Websites should comply with the school's guidelines for publications.***

St Michael's School App - EdTap

St Michael's PS App provides an alternative communication platform that allows instant messages/notifications containing information to be delivered directly to the user'smobile without requiring private contact information. The publishing of documents and messages can be restricted to specifically approved staff, ensuring that all conforms to school policies. Administrative functions are password protected, with communications and data storage both encrypted.

http://www.edtap.com/privacypolicy.pdf

SchoolMoney

SchoolMoney's secure online payments system, parents can pay for school dinners, uniform and school trips. This module also helps schools balance their books. By using the Paypoint system, families without online banking can make school payments in supermarkets, newsagents and post offices. With SchoolMoney's parental consent feature, primary contact details, medical information and permission for a range of activities can be supplied in an instant. SchoolMoney/Eduspot operate a safe and secure service using a fully encrypted, password sensitive SSL (Secure Sockets Layer) web service.

https://eduspot.co.uk/privacy-policy/

Cyber Bullying

Staff at St Michael's Primary School are aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of
school. This form of bullying is addressed within our school's Anti-Bullying Policy, Pastoral Care Policy as well as this E-Safety Policy.

Cyber Bullying can take many different forms and guises including:

- ***Email – Nasty or abusive emails which may include viruses or inappropriate content.***
- ***Instant Messaging (IM) and Chat Rooms- Potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.***
- ***Social Networking Sites – Typically includes the posting or publication of nasty or upsetting comments on another user's profile.***
- ***Online Gaming – Abuse or harassment of someone using online multi-player gaming sites.***
- ***Mobile Phones – Examples can include abusive texts, video or photo messages.***
- ***Abusing Personal Information – May include the posting of photos, personal information, fake comments and blogs or pretending to being someone online without that person's permission.***

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyberbullying, the following legislation covers different elements of cyber-bullying behaviour:

- ***Protection from Harassment (NI) Order 1997***
- ***Malicious Communications (NI) Order 1988***
- ***The Communications Act 2003***

At St Michael's Primary School, pupils are encouraged to report incidents of cyber-bullying to their parents and the school. If appropriate the PSNI may be informed to ensure that the matter is properly addressed and the behaviour ceases. The school will keep records of cyber- bullying.

Social Media

This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users.

Such software allows users to exchange resources, ideas, pictures and video. The majority of activity in these on-line social sites usually causes no concern. C2k filters outthese social networking sites and blocks attempts to circumvent their filters leaving it relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.

We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Appropriate information and indeed education will also be provided for our parents. Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Monitoring and Evaluation

The policy will be reviewed and amended in light of updated technologies or new DE Guidance.

Review Date

This Policy is to be reviewed annually.

Next Review Date: ***March 2023***

Review Comments

Review Date	Comments
May 2018	Draft Policy developed
September 2018	Policy Approved by Board of Governors
March 2021	Policy Updated

Appendix 1

ICT Code of Safe Practice for Staff (E-Safety Rules)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with the Principal.

- ***I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.***
- ***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 not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.***
- ***I will only use the approved, C2k, secure e-mail system for any school business.***
- ***I will ensure that personal data 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 Principal or Board of Governors.***
- ***Personal or sensitive data taken off site must be encrypted.***
- ***I will not install any hardware of software without permission***
- ***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 staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.***
- ***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 Principal.***
- ***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 e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.***

User Signature
I agree to follow this code of practice and to support the safe and secure use of ICT throughout St Michael's PS.

Signature …….
Date ……

Full Name…… (printed)

Appendix 2

Rules for Responsible Internet Use

The school has installed computers and Internet Access to help our learning. These rules will keep everyone safe and help us to be fair to others.

- ***I will access the system with my own login and password provided by the school;***
- ***I will only use the computer for school work and homework;***
- ***I will not bring in CDs or memory pens from outside school unless I have been given permission;***
- ***I will ask permission from a member of staff before using the internet;***
- ***I understand that the school will check my computer files and will monitor the Internet sites I visit.***

My parents/guardian and I have read the rules and I will abide by these rules to keep me safe.

Child's Name _____

Child's Signature _____

I have discussed the above rules with my child.

Parent's Name _____

Parent's Signature _____

Date _____

Photograph Permission

I/We consent for my/our child's photograph to be taken and used for display/theme purposes, for the School Newsletter and for the school website/app. When a photo is used on our school website/app, it will be displayed in line with our School E-Safety Policy. A photo will not be displayed with the child's name attached. I understand that on some occasions my child's photograph may also be included in the background of another child's photograph. In addition, I understand that on occasion my child may be taking part in events which may be publicised in the local press.

Signed_____ **Date**_____

Parent/Guardian

OR

I do not wish my/our child's photograph to be taken and used for display/theme purposes, for the School Newsletter and for the school website.

Signed_____ **Date**_____

Parent/Guardian

Thank you for completing the form. Please return to your child's class teacher as soon as possible.

Appendix 3

Google Meet EXPECTATIONS

Be on Time

Cameras On

Mics Muted at the start

Find a Quiet Space

Dress Appropriately

Use the Chat Feature to Ask Questions

Do not take Pictures or Screenshots

Raise Your Hand to Speak in Chat

Engage, Interact & Chat

Stay Safe in Remote Learning

Appendix 4

Google Classroom

Acceptable Use for Pupils

Be Responsible

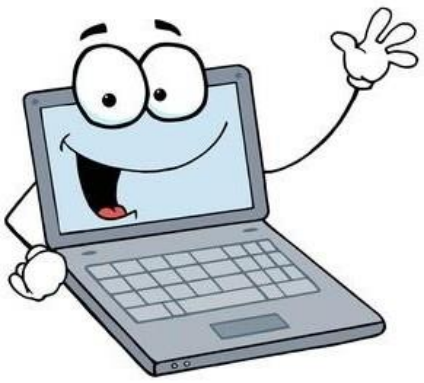
I will:

- use electronic devices, the Internet and the network for class and home learning assignments sensibly.
- use only my own account and follow the instructions my teacher has set me.

Be Respectful

I will:

- communicate online in a respectful manner.
- respect the work and privacy of others.



Be Safe

I will:

- keep my password and login information private.
- tell an adult if I read something on the Internet that makes me feel uncomfortable.
- refrain from sharing my personal information on the Internet.