Love **Determination** **Responsibility** **Respect** **Kindness** **Friendship** **Honesty**

Online Safety Policy

This Policy will be reviewed every year by the Curriculum Committee or, in the event of a change in legislation, earlier.

Updated October 2020

Signed

Head Teacher: Rosalind Owen

Chair of Governors: Elaine B. Bardwell

Date: 19 November 2020

Introduction
Every member of staff at St Michael's believes that online safety (e-safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, iPads, mobile phones, games consoles or any other internet enabled device.
Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Purpose
The purpose of the school's online safety policy is to:

- Make sure all staff and members of the school community understand how to be safe and responsible when using technology to ensure St Michael's is a safe and secure environment.
- Safeguard and protect all members of St Michael's community online.
- Raise awareness of the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear and easy to follow procedures to use when responding to online safety concerns that are known by all members of the school community.

Audience
This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and children and their parents/carers.
This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or iPads.

In conjunction with the following school policies:

- Safeguarding and child protection
- Anti-bullying
- Acceptable Use Policies
- Behaviour
- Consent for photographic images
- Personal, Social and Health Education (PSHE)
- Sex and Relationships Education (SRE)

Curriculum
Our curriculum has been planned to incorporate the latest government guidance.

Children are taught about the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app. (Department for Education, 2019).
This includes teaching the children about:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

Online safety is a whole school issue. At St Michael's we use the Education for a Connected World Framework to develop a rich, effective and developmental curriculum to support young people to be safe, healthy and thrive online.

There are 8 strands of the Connected World Framework and these are as followed:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

From September 2020, as part of the compulsory Relationships Education curriculum, children will be taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and know how to recognise and display respectful behaviour online. Teachers will address online safety and appropriate behaviour in an age appropriate way.

On-line safety is taught regularly in computing lessons and across the curriculum where appropriate. It is also in assemblies and events related to computing and online safety e.g. Internet Safety Day in February.

Key responsibilities for the school's leadership team (SLT)

- Develop and promote the online safety vision and culture to the whole school community in line with national and local recommendations.
- Ensure that online safety is viewed by the whole community as a safeguarding issue and proactively develop a robust online safety culture.
- Ensure there are appropriate and up to date policies and procedures regarding online safety.
- Ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content and which meet the needs of the school community whilst ensuring children have access to required educational material.
- Work with and support 123ICT in monitoring the safety and security of school systems and networks and ensure that the school network system is actively monitored.
- Ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and and the associated risks and safe behaviours.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Audit and evaluate current online safety practice to identify strengths and areas for improvement.
- Act as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Maintain a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.

Key responsibilities for the school's computing coordinator (Mr Lindars)

- Keep up to date with current research, legislation and trends regarding online safety.
- Lead on the development of the computing curriculum across the school and how online safety is covered and delivered.
- Disseminate information to all school staff.
- Coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Ensure the school's e-safety policy is up to date and reflects current legislation and practice.

Key responsibilities for all members of staff

- Contribute to the development of online safety policies.
- Read and adhere to the schools e-safety policy
- Take responsibility for the security of school systems and data that they work with.
- Have an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Model good practice when using new and emerging technologies
- Embed online safety education in curriculum delivery wherever possible.
- Identify individuals of concern and take appropriate action by following school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, internally and externally.
- Maintain a professional level of conduct in their personal use of technology, both on and off site and in accordance with the school's acceptable use policy.

Key responsibilities for staff managing the technical environment (123ICT)

- Provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Implement and maintain safe and secure systems and data management in partnership with the leadership team of the school.
- Ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Designated Safeguarding Lead (DSL).
- Ensure that the use of the school's network is regularly monitored and report any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Follow the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

Key responsibilities of children

- Contribute to the development of online safety policies.
- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.
- Take responsibility for keeping themselves and others safe online.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Abide by the school's Acceptable Use Policy for their age group.

Key responsibilities of parents and carers

- Contribute ideas to the development of online safety policies.
- Read and adhere to the school's online safety policy and acceptable use policies and support their children in doing the same (See Appendix 1 (KS1) and 2 (KS2)).
- Discuss online safety issues with their children, support the school's online safety approaches and reinforce appropriate safe online behaviours at home.
- Role model safe and appropriate uses of technology and social media.
- Be vigilant for changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Use school systems, such as Google Classroom, Tapestry and Class Dojo, and any other network resources, safely and appropriately.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Online Communication and Safer Use of Technology

Managing the school website

- The school will ensure that information posted on the school website meets the requirements required by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff and pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

Publishing images and videos online

Covered by the school's consent for photographic images document. This is available on the school website and from the school office.

Managing email

- Pupils are provided with an email through which they can access Google Classroom. These email accounts are only to be used for educational purposes.
- All members of staff are provided with a specific school email address to use for an official communication. Personal email addresses should not be used for professional communications.
- Any electronic communication which contains any content which could be subject to data protection legalisation will only be sent using secure and encrypted email.
- Members of the school community must immediately tell Mrs Owen if they receive offensive communication and this will be recorded in the school's safeguarding records.
- When communication is happening between parents and staff, for example through Tapestry and Class Dojo, staff will be encouraged to develop an appropriate work life balance when updating these platforms.

Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.

- All school owned devices will be used with appropriate safety and security measures in place.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will use the internet to enable staff and pupils to communicate and collaborate in a safe and secure environment.

Social Media *(to be read in conjunction with Acceptable Use Policy)*

- Expectations regarding safe and responsible use of social media will apply to all members of the school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, social networking sites (Class Dojo), multiplayer online games, apps, video/photo sharing websites and many others.
- All members of the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the school's senior leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding.

Official use of social media

At St Michael's we use the following platforms to communicate and engage with the community:

- Class Dojo (Whole school)
- Tapestry (Reception Class only)
- Google Classroom (Whole school)
- Parent Mail (Whole school)
- Twitter (Whole school)
- Library blogpost (Whole school)

Appendix 1

St Michael's C of E Primary School

Key Stage 1 Acceptable Use Policy

My name is _____

To stay **SAFE online and on my devices**:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my body, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep ~~**SECRETS**~~ or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** in front of a camera
10. I always check before **SHARING** personal information about me
11. I am **KIND** and polite to everyone

My trusted adults are:

_____ at school

_____ at home

LGfL DigiSafe Keeping children safe

Appendix 2

St Michael's C of E Primary School

Key Stage 2 Acceptable Use Policy

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend or sibling is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. Private information may be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult:

At school that includes _____

Outside school, my trusted adults are_____

Signed: _____ **Date: _____**