St. Michael's C of E Aided School

Back Lane, Aldbourne, Marlborough, Wiltshire SN8 2BP
Telephone: 01672 540434 Fax: 01672 541536
Email: admin@stmichaelsaldbourne.co.uk
Web: www.stmichaelsaldbourne.co.uk

Policy: Online Safety

Issue Date	Review Date	Document Owner(s)	Nominated Governor
7th December 2016	7th December 2017	B Everitt	Caroline Kaneen

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

St Michael's School 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, mobile phones or games consoles. We identify that the 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.
St Michael's identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of our online safety policy is to:

- Clearly identify the key principles expected of all members of the school community with regards to the safe and responsible use technology to ensure that St Michael's is a safe and secure environment.
- Safeguard and protect all members of the St Michael's community online.
- Raise awareness with all members of our school community regarding the potential risks as well as benefits of technology.
- To 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 procedures to use when responding to online safety concerns that are known by all members of the school community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

In addition, it 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 a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including, safeguarding and child protection, anti-bullying, behaviour, data security, image use and Acceptable Use Policies.

1.2 Writing and reviewing the online safety policy

This policy was written and will be reviewed by B. Everitt (DDSL and OSL).
The Designated Safeguarding Lead (DSL) is Mrs Judith Arkwright
The Online safety (e-Safety) lead for the Governing Body is Patrick Zebedee

1.3 Key responsibilities for our school community

1.3.1 The key responsibilities of the school management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole school community as a safeguarding issue and proactively developing a robust online safety culture.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring 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.
- Ensuring 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 the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead (Ben Everitt).

1.3.2 The key responsibilities of the Online Safety Lead are:

- Acting as a named point of contact (alongside DSL) on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Monitor the school's online safety incidents to identify gaps/trends and use this data to update the school education response to reflect need.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment (Oakford Technology) are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices – Laptops and desktops Bit Locker and iPads password protected.
- Ensuring that the schools filtering is applied and updated on a regular basis.
- Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the OSL/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.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring 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.

1.3.5 The key responsibilities of children and young people are:

- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Making every effort to attend school based events which promote online safety.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the school community.

2.2 Publishing images and videos online

- The school/setting will ensure that all images and videos shared online are used in accordance with the school image use policy.

- Parents/carers are asked not to post images (photos and videos) of pupils other than their own on social media sites unless they have the permission of parents of the other children pictured.
- At public events the school will display: 'We hope that you enjoy this event. Please be considerate of others when taking photographs. You are politely reminded that you should not post images on social media sites of pupils other than your own, unless you have permission from the parents of the other children pictured. Thank you for your support and understanding.'
- With regard to school managed social media platforms (PSA Facebook page) 'Any photographs have to be sent to Viv Lipscombe for approval before uploading – please email them to her and she will confirm approval'.

2.3 Managing email

- All members of staff are provided with a specific school email address to use for any official communication – it is expected that this, and not a personal email address, should be use for all school based communication.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email. Staff should direct all communication with parents through the 'admin@' address and avoid direct communication with parents using school email accounts.
- Emails sent to external organisations should be written carefully and authorised (if containing sensitive content) before sending.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 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.
- Esafety is taught as a part of Computing lessons (in accordance with the 'Switched On Computing' 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.

    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the St Michael's community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the St Michael's community will be encouraged to engage in social media in a positive, safe and responsible manner at all times (see parental agreement).
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the St Michael's community.
- Parents/carers are asked not to post images (photos and videos) of pupils other than their own on social media sites unless they have the permission of parents of the other children pictured.
- At public events the school will display: 'We hope that you enjoy this event. Please be considerate of others when taking photographs. You are politely reminded that you should not post images on social media sites of pupils other than your own, unless you have permission from the parents of the other children pictured. Thank you for your support and understanding.'
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media.

- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community (staff, children, parents, governors or volunteers).
- With regard to school managed social media platforms (PSA Facebook page) 'Any photographs have to be sent to Viv Lipscombe for approval before uploading – please email them to her and she will confirm approval'.
- The use of social networking applications during school hours for personal use is not permitted.

3.2. Official use of social media

- St Michael's official social media channels are:
    1. PSA Facebook Page
    2. School Vimeo Account
    3. Official 'blogs' set up by staff as a part of a computing unit or to communicate events of a residential trip.
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be assessed approved by the head teacher and governors.
- Staff will use school provided email addresses to register for and manage any social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear and transparent.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Official social media sites or blogs will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence (passwords will be recorded in the 'password book'.
- The following will be posted on the PSA Facebook page, 'This group is endorsed by St Michael's School, run by the PSA and available to all current members of the school. It is a private group, meaning that only member will be able to see what is posted here. It is intended as an informal place to share, or check on, information relating to school life. It can also be used as a way of inviting people for social events. We welcome your questions and look forward to seeing our community flourish. Please note that this page is not intended as a forum for concerns or feedback about the school itself. These are welcomed by the school, but should be addressed towards the teachers or head teacher directly, and so comments that fall into this category, will be removed by administrators of the page without warning. Also any photographs have to be sent to Viv Limpscombe for approval before uploading – please email them to her and she will conform approval. Thank you for being part of our school community and we hope you find this page a useful resource.'

3.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (school provided email address or phone numbers).
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted.
- Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of St Michael's on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

3.4 Pupils use of social media

- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any official social media activity involving pupils will be moderated by the school where possible.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.
- Where appropriate, children will be asked, as part of esafety teaching, which sites they use. Their teacher will make every effort to create a bespoke esafety scheme of work to demonstrate the specifics of how to set security controls and to use the platform safely. Staff will receive training on how best to achieve this.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of St Michael's community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in the school's Acceptable Use policy.
- St Michael's recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

4.2 Possible Statements:

- All use of personal devices and mobile phones will take place in accordance the school's Acceptable Use Policy
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items..
- Mobile phones and personal devices are not permitted to be used in front of the children.
- All members of the St Michael's community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

- All members of the St Michael's community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- Schools devices must always be used in accordance with the Acceptable Use Policy.
- When on trips (including residentials) contact with parents should be conducted through the school or using the school mobile phone. Personal devices should not be used for this unless extreme circumstances prevail.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Should a pupil need to bring a personal device into school, it should be immediately handed to the school office where it can be safely stored until the end of the day.
- If members of staff have an educational reason to allow children to use their personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.5 Staff use of personal devices and mobile phones:

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose. If this is unavoidable, images will be deleted at the earliest possible moment.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school acceptable use policy. Those who spend more than a brief visit to the premises will need to sign an acceptable use policy. This includes, but is not limited to: staff, governors, volunteers, admin, music teachers and catering staff.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- St Michael's is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- Oakford technology will run a weekly Filtering Check and pass details of this to the OSL.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

5.2 Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils – this will be taught through the 'Switched on Computing' scheme and also through PSHE.
- Education about safe and responsible use will precede internet access.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.
- Acceptable Use expectations needs to be signed and posted in all classrooms.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

- External support will be used to complement and support the schools internal online safety (e-Safety) education approaches e.g. guest speakers where appropriate.

6.2 Engagement and education of staff

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.

6.3 Engagement and education of parents and carers

- St Michael's recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly by Oakford Technology.
- Virus protection will be updated regularly (by Oakford Technology).
- Personal data taken off site will be encrypted by BitLocker.
- Unapproved software will not be allowed in work areas or attached to email.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

All users will be informed not to share passwords or information with others and not to login as another user at any time.

- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From year 1 all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- As the children move through the school, the password is change to develop its complexity.

7.3 Filtering and Monitoring

- The school (in partnership with Oakford Technology) will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- All users will be informed that use of school systems can be monitored.
- The school uses educational filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.
- The school will work with Oakford Technology to ensure that filtering policy is continually reviewed.
- Breaches of filtering will be reported to the OSL (B.Everitt) who will in turn inform Oakford who will update the Filtering Service.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.

- Any material that the school believes is illegal will be reported to appropriate agencies immediately.

7.4 Management of applications (apps) used to record children's progress (2build a profile in EYFS)

- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft (iPads and the App are pin protected).

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc (covered within CP training for all staff).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Wiltshire Safeguarding Children Board thresholds and procedures.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- Staff will be informed of the whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- St Michael's ensure that staff and age appropriate children are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- St Michael's views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (J Arkwright).

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- St Michael's will ensure that staff are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- St Michael's views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- St Michael's will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- If the school are made aware of an incident of IIOC, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Wiltshire Police.
- All staff will have taken part in PREVENT training.

9.5. *Responding to concerns regarding cyberbullying*

- Cyberbullying, along with all other forms of bullying, of any member of St Michael's community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded in the book stored in the school office.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.