St. Michael's CE Primary School, Sandhurst

Online Safety Policy

Issue: October 2023
Review Date: October 2024

School Vision
As a school community, we aspire to develop life-long learners who have the confidence to explore the world around them and grow as unique individuals. We provide a safe family environment, inspired by Christian values, in which the flourishing of each enables the flourishing of all.

'This little light of mine, I'm going to let it shine!'

'Let your light shine before others, so that they may see your good works and give glory to your Father who is in heaven.' Matthew 5:15

Contents:

1. Introduction
In St. Michael's Primary School the welfare and well-being of our pupils is paramount. This policy on the use of technology in school, and in some cases outside of school as well, has been drawn up in the best interests of pupil safety and staff professionalism.

This policy related to the Computing policy, and other policies including those for Safeguarding, Behaviour, Anti-bullying, core subject policies (English, Mathematics and Science), Foundation Subjects Policy and Personal, Social, Health and Emotional Education (PSHE). It has been agreed by the senior management and approved by governors and will be reviewed annually.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

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

St Michael's first point of contact for Online Safety is:
Stuart Bevan (Headteacher and Safeguarding Lead)

Support provided by:
Olivia Leatherbarrow (Computing Subject Leader) and TSI

2. Importance of the internet

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience to enable them to engage effectively in the modern world. Internet use is now part of the statutory curriculum and a necessary tool for learning.

The purpose of internet use in school is to:

- Raise educational standards
- Promote pupil achievement
- Support the professional work of staff
- Support the school's assessment process
- Enhance the school's management functions and administration systems
- Enable effective communication between the school, parents and outside agencies
- Develop responsible and mature approaches to internet use
- Enable users to evaluate internet information effectively
- Enable users to take care of their own safety and security.

Benefits of using the internet in education include:

- Access to world-wide educational resources, including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Access to learning wherever and whenever convenient
- Access to experts in many fields for pupils and staff
- Vocational, cultural, social and leisure use in libraries, clubs and at home
- Professional development for staff through access to National developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support, including remote management of networks and automatic system updates
- Exchange of curriculum and administrative data with Bracknell Forest Borough Council and the Department for Education (DfE).

Use of the internet to enhance learning

Technology is an ever growing part of our everyday lives, both in school and at home. In order to utilise the many educational and social benefits of new technologies, learners need opportunities to create, collaborate and explore the digital world. This can, however, mean that users occasionally encounter risks and may be confronted with inappropriate material. Managing this online safety risk depends on effective practice in each of the following areas:

- A comprehensive, agreed and implemented Online Safety Policy
- A secure, filtered broadband network
- A school network that complies with the National Education Network standards and specifications
- Education for responsible computing use by staff and pupils, including protocols for staff and children on dealing with inappropriate content.

3. Managing Information Systems

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the international scale and ever-changing nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school

computer. Neither the school nor Bracknell Forest Borough Council can accept liability for the material accessed, or any consequences of internet access.

Risk Assessment

- Methods to identify, assess and minimise risks will be reviewed regularly
- The SLT will ensure that the Online Safety policy is implemented and complied with via the Acceptable Usage Policies (see appendices), staff training and regular checks
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Access is strictly forbidden to any websites that involve pornography, violence, racism, gambling or financial scams.

Filtering

- The school will work in partnership with parents, the LA, and the Internet Service Provider (ISP) to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Online Safety Lead
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk)
- TSI , will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

Security

It is important to review the security of the whole system, from user practice to ISP:

- The school computing systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the LA
- Personal data relating to pupils may not be sent from or to personal e-mail accounts. Instead, all staff must use secured school user accounts to send data over the internet
- Portable media such as memory sticks and portable hard drives may not be brought into school without specific permission. It will be the user's responsibility to ensure that a virus check is conducted if they deem it necessary
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or any e-mail attachments
- Workstations will be secure from casual mistakes by the user
- The network manager will ensure that the system has the capacity to take increased traffic caused by internet use
- All users must act in accordance with their Acceptable Use Policy
- Good password practice is encouraged including logout after use and not giving passwords to others
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Internet access

Internet use is part of the statutory curriculum and entitlement for all responsible and mature users. Government guidance suggests that, in primary schools, all pupils are granted internet access as a class group with full supervision of all pupil use.

- Parents carers will be informed that pupils will be provided with supervised internet access
- Staff, student teachers or other staff undertaking placements at the school will sign the 'Acceptable Use Policy: Internet Use (Staff)' (Appendix A) before using the internet on any school computing resource
- The school will keep an up-to-date record of all staff and pupils who are granted internet access
- At Foundation Stage and Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved online materials depending on the nature of the task
- Parents are required to give permission for their child to use the internet within school and support the school in Online Safety when their child is at home.

E-mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, unmediated email access carries many risks such as cyber-bullying, transmission of viruses, contact with inappropriate material and identity theft. Therefore, use of e-mail in school must be carefully monitored to ensure safety and security.

- Pupils may only use approved e-mail accounts on the school system
- Whole-class or group e-mail addresses should be used, unless discussed with the Computing Subject Leader prior to the set-up of singular e-mail addresses
- Pupils are taught that they should immediately tell an adult if they receive offensive e-mail
- The forwarding of chain letters is not permitted
- Personal email or messaging between staff and pupils must not take place
- Pupils must not reveal details of themselves, others or the school in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone
- E-mail by staff that is sent to an external organisation should be written carefully and authorisation sought if considered necessary. Staff are responsible for sending their own e-emails which uphold the polices of the school
- Staff must use secured school user accounts to send any data about pupils over the internet. This includes levelling data, reports, IEP's, SEND referral information and information relating to the personal circumstances of pupils or their families.

School Website

Websites can celebrate pupils' work, promote the school and publish resources for pupil use. Whilst there are many ways to obtain information about schools and pupils, a school's website can be accessed publicly. Publication of information should therefore be considered from a security viewpoint.

- The point of contact on the website should be the school address, school e-mail and telephone number
- Staff or pupils' home information will not be published
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used in association with photographs. No child will be clearly identified with a name and a year group, unless as part of a group (e.g. Year 5/6 Football Squad: Child [insert name], Child [insert name] etc.)
- Parents will be informed about the digital image procedures and given the option to refuse consent for their child to appear in digital images published on the school website
- The Deputy Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate

- The website should comply with the school's guidelines for publications
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

Photographic, video and audio technology

Digital image technologies and audio recordings can be very powerful learning tools. It should be noted at that this point that 'digital images' refer to both digital photographs and digital videos. Video conferencing, audio recording (e.g. podcasting, digital video and digital cameras) may all be used in the classroom to enhance learning activities. The following statements are included to prevent misuse and protect users and subjects:

- The downloading of audio or video files is only permitted when being downloaded onto school computing hardware (e.g. laptops), when the user has gained prior permission from the network manager/IT Technician
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken
- Pupils should always seek the permission of their teacher before making digital image or audio recordings within school
- Staff, student teachers or other staff undertaking placements at the school will sign the Acceptable Use Policy: Digital Images (Staff) (Appendix B)
- Staff may take digital images using the class or school camera to support school trips and curriculum activities, including assessment and record keeping
- Staff will not use personal equipment (e.g. mobile phones, digital cameras or video cameras) to take digital images of any pupils without permission from a member of the SLT for a specific event or activity (e.g. recording the summer production or attending a sporting event with a professional camera). If staff use personal devices, they are required to delete any school-related photos as soon as they are uploaded to school hardware (e.g. laptops/network). Posters in the classrooms will remind staff of this
- Staff may use and store digital images and audio recordings needed for professional purposes on laptops and computers off the premises. However, images must be free of any information that would enable identification and tracking of children (e.g. adding names to photographs)
- It is not appropriate to use digital image or audio devices in situations/places where a child may be captured in an unsuitable state (e.g. in the toilet, whilst changing for P.E., in changing rooms etc.)
- Care should be taken when capturing digital images to ensure that all pupils are appropriately dressed
- Staff and pupils are aware that their use of technology may be monitored for safety
- Any images of children used in school training and promotional materials (e.g. websites and prospectus) will not include full names of the children
- Parents/carers will be informed about the school's digital image procedures and given the option to refuse consent for their child to appear in digital images taken by the school. It is the responsibility of parents/carers to inform the school if they wish to change their decision
- The school will keep an up-to-date record of all pupils who do not have parental consent to appear in digital images
- All staff must sign the Acceptable Usage Policy: Digital Images (Staff) (Appendix B) before using any school computing resource
- The school's policy regarding digital images will be reviewed regularly in consultation with the LA and LSCB, with regard to security
- Parent are permitted to use mobile phone cameras to take pictures of their own child/children at class assemblies, school productions and school sports events. However, this privilege could be withdrawn if deemed to be inappropriate.

Social networking and personal publishing

The internet has emerging online spaces and social networks which offer great potential for education. Collaboration tools such as discussion forums and newsgroups are exciting methods for pupils and teachers to share information and opinions. Blogs may provide commentary or news on a particular subject and can be used as a class diary to chronicle learning activities. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. Unfortunately, many of these online spaces and tools allow individuals to publish unmediated content and therefore carry an e-safety risk of cyber-bullying and inappropriate contact. To protect against this risk, the following statements will be applied:

- Newsgroups or other open forums will not be made available to pupils unless an educational requirement for their use has been demonstrated
- The school will block access to social networking sites for pupils, although staff may use these for educational purposes
- With regard to social networking, pupils will be permitted to access and use school accounts if supervised by a member of staff, who takes full responsibility for the content seen and posted
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include: real name, address, mobile or landline phone numbers, school attended, instant messenger and e-mail addresses, full names of friends, and specific interests etc.
- Pupils should be advised not to place personal photos on any social network space
- Pupils should be advised not to publish specific and detailed private thoughts about themselves or others
- Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing information once published
- Pupils should be advised on security of personal internet spaces and encouraged to set passwords, invite known friends only and deny access to unknown individuals
- Teachers, parents/carers and pupils should be aware that bullying can take place through social networking and messaging and taught how to address these issues
- Personal use of social networking sites by staff is not forbidden, but guidelines for safe use are laid out in the Acceptable Usage Policy: Internet Use (Staff) (Appendix A) and will be adhered to
- Advice regarding the use of forums, social networking sites and messaging facilities will be provided for parents/carers through the school website.

Emerging Computing Applications (Apps)

Many emerging communication technologies offer the potential to develop new teaching and learning tools. However, the rate at which computing is changing means that it is very difficult to identify potential threats before pupils have started to experience and use a new service or technology. It is therefore crucial that pupils are taught to identify potential risks and to apply Online Safety principles in a range of situations so that they are likely to respond appropriately to new situations.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones will not be used during lessons or formal school time unless, due to exceptional circumstances, specific permission has been granted to the family, in which case the phone will be kept in the school office or by the class teacher during school hours
- Pupils in Year 5 and 6 only may bring a mobile phone to school. The phone must be turned off or placed on 'silent mode' and kept in the school office throughout the day. The school governors and staff recognise that many Year 5 and 6 pupils are becoming independent in their travel to and from school and wish to formally support parents in their children's safeguarding. Mobile phones in school are solely the child's responsibility

- Mobile phones brought in without permission from the school are the owner's responsibility and may be confiscated by a staff member. If this occurs, the parents will be notified via a phone call or letter.

4. Education in Online Safety

Whilst managing information systems forms an essential part of protecting internet users, it is now recognised that Online Safety risks are posed more by behaviours and values online than the technology itself (Becta, 2009). Therefore, empowering learners to develop safe and responsible online behaviours is a priority if they are to be protected whenever and wherever they go online.

Recognising the risks

To enable children to be safe online, education must be provided which helps to raise awareness and understanding of the opportunities and threats of technology use, through the provision of information, training, policy and procedure. Education which helps children to recognise and avoid unsafe online behaviours empowers users with the skills, knowledge and confidence they need to embrace new technology safely.

- Lessons giving direct Online Safety teaching and instruction are included in the PSHE and Computing programme of study for KS1 and KS2, covering both home and school internet use
- Pupils will be taught what internet use is acceptable and what is not (e.g. in relation to cyber-bullying)
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening
- Pupils will be taught to avoid hardware becoming infected with and transmitting computer viruses
- Pupils will be taught to keep personal information private to protect them from online predators and identify theft
- Pupils will be taught how to report concerns and contact with inappropriate material
- Children will be aware of their Acceptable Use Policy and this will be displayed by all computers.

Evaluating internet content

When learning to use the internet, the quantity of information retrieved during searches can be overwhelming. Users may also experience difficulty in determining the origin and accuracy of information, as the contextual clues present with books or TV may be missing or difficult to read. In Key Stage 1, offering a few good sites will often be much more beneficial than allowing pupils to search the whole web, whilst older pupils must learn how to distil the meaning from the mass of information through guidance and modelling of appropriate research techniques. Guided use will also reduce the opportunity pupils have for exploring sites that are inappropriate

- Internet access will be planned to enrich and extend learning activities
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity
- In Foundation Stage and KS1, younger pupils may be guided to appropriate websites and taught search skills within restricted online environments
- In Key Stage 2, pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Respecting Copyright
In most instances, pupils will be judging appropriate material but will need to select relevant sections. They will be helped to understand that unselective copying is of little value and the reproduction of copyright materials can be a criminal offence, equivalent to theft.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work
- The school will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.

5. Online Safety incidents
Despite the comprehensive online safety measures in place, there may still be occasions when on line safety incidents occur. As such, there are clear guidelines for responding to these incidents, such as cyber-bullying, transmission of viruses, security breaches and access to inappropriate materials.

Accidental access to inappropriate content

- Inappropriate content is defined as any access to materials which contain violent, harmful or sexual content and/or reference to cultural, racial or homophobic discrimination
- All incidents of accidental access to inappropriate materials are immediately reported to the named Online Safety lead using the Online Safety Incident Log (Appendix D). The site URL is recorded for inclusion in the list of blocked sites
- Any access to inappropriate material is formally documented in school and then passed on to the school's Internet Service Provider (ISP) to investigate further
- Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk)
- Access to the reported sites can be immediately blocked by the Online Safety Lead using RM Safety Net+ software
- Filtering is regularly checked by network manager, Internet Service Provider (ISP) and South East Grid for Learning (SEGfL). ISP monitors standards by producing reports of blocked sites and internet usage
- Any inappropriate content accessed whilst using resources posted on the school's website must be reported to the school and all links will be removed.

Suspected Breach of the School's Acceptable Use Policy (AUP)
The school may exercise its right to monitor the use of the school's computer systems. This includes access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Deliberate Breach of the School's Acceptable Use Policy (AUP)

- All online safety incidents are promptly reported to the named Online Safety Lead. The incident will then be recorded in the Online Safety Incident Log (see Appendix E) and be escalated following the school's Online Safety Incident Escalation Flowchart (see Appendix F)
- The incident log will be reviewed termly by the Online Safety committee
- All incidents of misuse (from staff or pupils) will be promptly reported to the Headteacher or Online Safety/ Computing Subject leader. Different incidents will require different responses, depending on the nature of the event. Sanctions may include:
  - *Disciplinary action*
  - *Interview/counselling by Headteacher or appropriate agency*
  - *Informing parents/carers*
  - *Removal of internet or computer access for a specified period*

- Involvement of outside agencies specified by the Escalation Flowchart

- Incidents of cyber-bullying will be dealt with in line with the school's Anti-bullying policy
- The Headteacher will establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence
- Parents/carers and pupils will need to work in partnership with staff to resolve issues.

6. Involvement of the school community

Online Safety is primarily a safeguarding issue, so anyone with responsibility for the welfare of children and young people needs to be involved, including the children themselves.

Involvement of staff

- All staff will receive a copy of the Acceptable Usage Policy: Internet Use (Staff) (Appendix A) and will be required to read and accept the terms outlined before using any internet resources at school
- All staff will receive a copy of the Acceptable Usage Policy: Digital Images (Staff) (Appendix B) and will be required to read and accept the terms outlined before using any photographic equipment in school
- All staff, including teachers, support staff, supply staff and administrative staff will be provided with the school's Online Safety policy and have its importance explained
- All new staff will be provided with a copy of this policy on joining the school and will be taken through the key parts of the policy as part of their induction
- All teaching and support staff will receive training in online safety issues as required and are expected to take personal responsibility for their professional development in this area
- All teachers will be involved in delivering age online safety instruction to their pupils
- All staff are aware of their responsibilities to report any misuse or suspected misuse of the computing systems in school
- All staff are made aware that internet traffic can be monitored and traced to an individual user
- The monitoring of internet use is a sensitive issue. Staff who operate monitoring procedures will be supervised by the SLT
- Breaching this online safety policy may result in disciplinary action being taken and access to computing being restricted or removed.

Involvement of pupils

- All pupils are made aware of their rights and responsibilities when using computing systems through the Pupils' Acceptable Use Policy (see Appendix C)
- The Pupils' Acceptable Use Policy (see Appendix C) is drawn up in consultation with pupils through class discussion and School Council
- The Pupils' Acceptable Use Policy is posted in all rooms where computers are used and children's attention drawn to relevant items during teaching
- Instruction in responsible and safe use should precede internet access and be revisited regularly through the taught Computing curriculum
- Pupils' attention is drawn to displays around the school which reinforce online safety messages
- Pupils will be informed that their internet use will be monitored
- School Council have contributed to and agreed upon the Acceptable Usage Policies (Appendix C) to encourage safe practices within the home.

Involvement of parents

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet at home. Steps have been taken to improve parent

understanding of the risks of internet use and develop the use of safe practices within the home as well as at school.

- Parents are required to give permission for their child to use the internet within school and support the school in online safety when their child is at home
- A partnership approach with parents will be encouraged to ensure a shared understanding of online safety advice between staff, pupils and parents. This may include training events, demonstrations, information leaflets and suggestions for safe internet use at home
- Online safety issues will be handled sensitively to inform parents without undue alarm
- Advice on filtering systems will be made available to parents
- Access to educational activities and advice on appropriate leisure activities and responsible use of the internet will be offered to parents through the school website.

Involvement of community

Internet access is available in many situations in the local community, including after-school child care facilities and clubs/organisations such as Cubs/Brownies. Ideally, young people would encounter a consistent policy to internet use wherever they are. Although this may not always be possible, attempts will be made to communicate our online safety vision with community partners.

- The school will liaise with organisations associated with the school to establish a common approach to online safety
- The school will be sensitive to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice
- Any organisation using the school's computing systems and network will be expected to comply with the online safety policy
- All staff and children using the school's computing systems will be required to understand and sign an Acceptable Use Policy, appropriate to their age, role and computing use.

Wider personal use of digital communications

While the section above refers to communications between staff / volunteers and children /young people consideration should also be given to how the use of digital communications by staff and volunteers in their private lives could have an impact on the reputation of themselves and the group. Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as "friends" on social networking profiles and which information / photos are available to those friends.
- Privacy settings should be frequently reviewed
- The amount of personal information visible to those on "friends" lists should be carefully managed and users should be aware that "friends" may still reveal or share this information.
- "Digital footprint" – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them. A large proportion of employers engage in searches of the internet when selecting candidates and are influenced by what they find.

Appendix A

Acceptable Usage Policy: Internet Use (Staff)

To ensure that staff are fully aware of their responsibilities with respect to use of the school computer network and internet facilities, they are asked to sign this acceptable use agreement.

I will:

- Take responsibility for my own use of technologies, ensuring they are used safely, responsibly and legally
- Take an active part in online safety education and training and promote online safety with pupils to support the development of a responsible attitude towards using technology
- Report any known misuse of technology and online safety incidents (e.g. the viewing of inappropriate material or cyber-bullying) to the online safety lead. This information will then be passed on through the appropriate channels (see Appendix F)
- Report any failings in network filters (e.g. inappropriate material being accessed) to the computing Technician using the E-Safety Incident Log (Appendix E) and reported to the Online Safety officer
- Ensure that all electronic communications sent through the school network are compatible with my professional role and contain appropriate content and language
- Respect copyright of materials
- Scan any removable devices (e.g. USB drives; CD-ROMs) used on the school network for viruses before opening/using.

I will not:

- Install any software or hardware without permission from the online safety lead or TSI
- Send information about pupils to or from personal e-mail address. This includes: tracking data; reports; IEPs/EHCP and other SEND referral information; and information relating to the personal circumstances of pupils or their families
- Disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system
- Post anonymous messages or forward chain letters
- Use personal equipment (e.g. digital cameras, video cameras or mobile phones) to take digital images of any children and families associated with St Michael's Primary School, unless the personal equipment has been checked and certified as suitable by the e-safety officer or agreed by a member of SLT. I will remove all media from personal devices as soon as they are uploaded to school hardware (e.g. laptops or the school network).

I understand:

- That St Michael's Primary School reserves the right to monitor my network and examine or delete any files that may be held to ensure the safety of all staff and children
- That the network is the property of St Michael's Primary School and agree that my internet activity must be compatible with my professional role or the children's education
- That deliberate misuse of the network (e.g. hacking, the circulation of virus or interfering with safety controls) is forbidden
- That use of the network to access inappropriate content (such as pornographic, racist, homophobic or offensive material) is forbidden and would result in disciplinary action
- That use of the network for personal financial gain, gambling, political purposes or advertising is forbidden and would result in disciplinary action.

Social Networking

Social networks are rapidly growing in popularity and used by all ages in society. However, as educators, we have a professional image to uphold and how we conduct ourselves online helps determine this image. The use of social networking sites, such as Facebook, Twitter and Instagram, is

not forbidden, but staff are advised to treat with caution if used. The following recommendations are suggested to support safe use:

- Do not post personal information about yourself, e.g. address, phone number
- Never post any pictures of yourself or pupils at school; this includes pictures of classrooms and the school grounds
- Use the privacy features provided on the site to restrict access of strangers and those who you have not specifically selected as 'friends' to your profile
- Adjust your privacy settings so only your online 'friends' are able to view your photos and any photos in which you are 'tagged'
- Do not accept or initiate any friend requests with pupils associated with the school. This is not only to protect your information, but also that of colleagues which may feature on your profile
- Staff must not accept or initiate any friend requests with parents associated with the school unless a member off staff has specific needs to be part of the same Facebook group as parents- i.e. if their child is in the same class as that of a parent's child. This is not only to protect your information, but also that of colleagues which may feature on your profile
- All Staff are to ensure that Facebook is set to private. Staff must regularly check privacy settings especially after any changes to Facebook logins have been reset
- Do not discuss pupils, parents, colleagues or the school itself on social networking sites
- Use a strong password (i.e. more than 7 characters made up from a mixture of letters, numbers and other characters) and change it regularly.

Failure to behave in accordance with the terms of this agreement may result in disciplinary action.

Staff member's name:

Signature:

Date:

Appendix B

Acceptable Usage Policy: Digital Images (Staff)
(both still and moving digital imagery)

To ensure that staff are fully aware of their responsibilities with respect to use of digital images, they are asked to sign this acceptable use agreement.

- I understand that all photographs taken of children and families associated with St Michael's Primary School, both in school and outside on visits, are the property of St Michael's Primary School
- I understand that all digital images will be taken with St Michael's Primary School cameras and/or stored on memory cards purchased by St Michael's Primary School agreed with SLT or Computing Technician.
- I understand I may not use personal equipment (e.g. digital cameras or video cameras) to take digital images of any children and families associated with St Michael's Primary School, without specific written permission from a member of SLT for a specific event or activity (e.g. recording the summer production or attending a sporting event with a professional camera).
- I understand digital images needed for professional purposes may be used and stored on laptops and computers off the premises. The photographs need to be free of any information that would enable identification and tracking of children (e.g. adding children's full names to photographs).
- I understand I must only take responsible digital images of children (e.g. children will be dressed appropriately).
- I understand that images may not be distributed outside the school network without the permission of the parent/carer and/or a member of SLT.
- I understand and agree that St Michael's Primary School may monitor my technology use to ensure the safe use of digital images of children and families associated with the school.
- I understand and agree that any photographs of children to be used in St Michael's Primary School training and promotional materials and on websites will not include the full names of the children.
- I understand that I may only take digital images of children who have been granted parental permission.

Staff member's name:

Signature:

Date:

Appendix C

EYFS and KS1 Acceptable Usage Policy for home and school

- I will only use a computer or tablet if there is an adult with me.
- I will tell an adult if I see anything I don't like or am confused by.
- I will only send friendly and polite messages to people I know.
- I will not touch a computer or tablet if my hands are dirty or wet.
- I will not click on things an adult hasn't shown me how to use.
- I will not turn the computer on or off unless an adult has agreed.
- I understand that these rules will help to keep me and my family safe.
- I understand these rules.

Key Stage 2 Acceptable Usage Policy for home and school

- I will ask permission before using the internet.
- I will only open and delete my own files.
- I will only email and open email attachments from people I know, or who my teacher has approved.
- I will make sure that all computing contact with other children and adults is polite and sensible.
- I will tell my teacher right away if I come across any information which I don't like or makes me feel uncomfortable.
- I will not give out personal information like my name, address, telephone number, picture or the name and location of my school without permission.
- I will not agree to get together with someone I "meet" online.
- I will not give out my computing passwords to anyone other than my teacher (not even to my best friends).
- I will not download or install any software.
- I will not use USB drives or other external devices from outside school unless my teacher says I can.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not reply to messages that are mean or make me feel uncomfortable. Instead I will tell my teacher right away.
- I will not upload or post any pictures of other children on to the internet including social networking sites.
- I understand that my teachers can check what I am doing to make sure I am behaving responsibly and staying safe.

Appendix D

Online Safety Incident Log

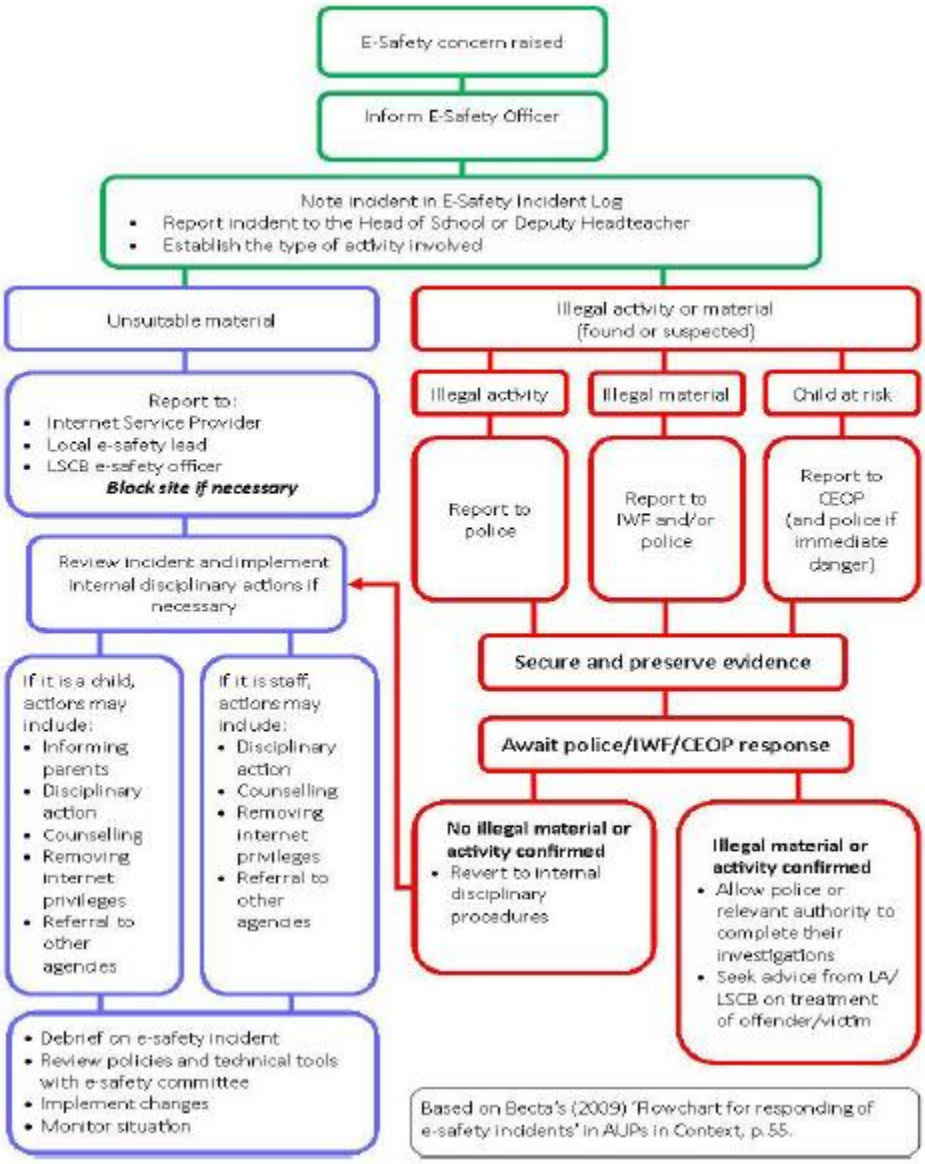
Details of ALL Online safety incidents are to be reported to and recorded by the named Online Safety lead All incidents will be escalated according to the Online Safety Incident Response Flowchart (see Appendix F) in line with Becta advice.

The incident log will be monitored termly by the Headteacher and the e-safety committee.

Date & Time:	Name of pupil or staff member:	Male or Female:	Room & device number:	Details of incident (including evidence):	Actions and Reasons:

Appendix E

E-safety Incident Escalation Flowchart



Definitions:
LSCB: Local Safeguarding Children Board
IWF: Internet Watch Foundation
CEOP: Child Exploitation and Online Protection Centre