St Michael's Prep School

Online-Safety Policy (Previously e-Safety Policy)

Date of Last Review:	December 2018	Review Period:	As required
Date of Next Review:	September 2019	Owner:	JBO, GBA, JAI
Type of Policy:	Welfare, Health and safety	Board Approval	Scheduled for January 2019

Adopted: December 2018

Policies which inform this document include: -

- Safeguarding Policy
- Behaviour and Reward Policy
- Code of Conduct

1. Rationale

St Michael's Prep recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good Online-Safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online-Safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings or for grooming for radicalisation. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of Online-Safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school

community can use as a reference for their conduct online outside of school hours. Online-Safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Behaviour Policy.**

This policy has regard for the Standard guidelines for all schools published by KCC in January 2016 using the template on the KELSI website http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/Online-Safety and the template provided by Optimus Education.

This policy takes into account guidance published

- Working Together to Safeguard Children (March 2015)

  https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

- Keeping Children Safe in Education (September 2018)

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741315/Keeping_Children_Safe_in_Education_2018__Part_One__14.09.18.pdf

2. End to End Online-Safety

Online-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband currently provided by the KLZ (Kent learning Zone) including the effective management of Websense filtering.
- National Education Network standards and specifications.
- Staff Training

3. Further Information

Kent County Council Education & Safeguarding Team:

Principle Officer of Education & Safeguarding Team	Kel Arthur
Area Safeguarding Advisor	Rebecca Avery
Kent County Council Online-Safety Officer	Rebecca Avery – rebecca.avery@kent.gov.uk /

esafetyofficer@kent.gov.uk

W: 03000 415 788

Mob: 07789968705

http://www.kent.gov.uk/education-and-children/protecting-children/onlinOnline-Safety

Kent Community Network Helpdesk	03000415797 / 03000418707
ASK curriculum ICT staff	01622 203800
Online-Safety materials and links	www.thinkuknow.co.uk
Curriculum Online-Safety advice	as above and www.kidsmart.org.uk/beingsmart https://www.getsafeonline.org http://www.saferinternet.org.uk/ https://www.ceop.police.uk/

4. Roles and Responsibilities

The school Online-Safety Coordinator is Jamie Booth

Signature: .....

The designated member of the Governing Body responsible for Online-Safety is Cameron Kiggell

Signature: .....

Governors

Governors are responsible for the approval of the Online-Safety Policy and for reviewing the effectiveness of the policy by reviewing Online-Safety incidents and monitoring reports. Online-Safety falls within the remit of the Governor responsible for Safeguarding. The role of the Online-Safety Governor will include:

- Ensure an Online-Safety Policy is in place, reviewed every three years (or sooner in the event of a change to KCSIE) and is available to all stakeholders.
- Ensure that there is an Online-Safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to.
- Hold the Headteacher and staff accountable for Online-Safety

Headteacher and SLT

The Headteacher has a duty of care for ensuring the safety (including Online-Safety) of members of the school community, though the day-to-day responsibility for Online-Safety will be delegated to the Online-Safety Co-ordinator. Any complaint about staff misuse must be referred to the Online-Safety Coordinator at the school or, in the case of a serious complaint, to the Headteacher.

- Ensure access to induction and training in Online-Safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.

- Work in partnership with the DfE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the Online-Safety Co-ordinator.

Online-Safety Coordinator:

- Leads Online-Safety meetings.
- Work in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of Online-Safety incidents and creates a log of incidents to inform future Online-Safety developments,
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the Governing Body & Headteacher to provide an annual report on Online-Safety.

ICT Manager / Technical Staff - The ICT Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required Online-Safety technical requirements and any relevant body Online-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with Online-Safety technical information in order to effectively carry out their Online-Safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; Online-Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

ICT Strategy Lead is responsible for ensuring that

- all developments to the infrastructure, service providers and systems are taken following appropriate security risk assessments and are GDPR compliant

Staff:

- 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 online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- 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
- Taking personal responsibility for professional development in this area.

Parents

- Reading the school/setting 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 new and emerging technology.
- 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.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Pupils

- Contributing to the development of online safety policies.
- 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.

5. Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and Online-Safety guidelines, are displayed in the ICT rooms and offices. An Acceptable Use agreement is periodically onscreen for all users to sign that they agree to. Online-Safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

6. Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Supervision guidelines appear below;

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.
At Key Stage 3 pupils will be appropriately supervised when using technology, according to their ability and understanding.

Some of the benefits of using ICT and the Internet in schools are:

For pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.
- Access to online learning platforms in Languages, Espresso and Maths.

For staff:

- Professional development through access to CPD online package from Optimus/ Veale Wazbrough Vizards etc
- Access to national developments, educational materials and examples of effective curriculum practice and classroom strategies through TES online.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

For parents:
By using email for school communications it speeds up the process and makes it environmentally responsible. On our new website increased engagement is also possible.

7. Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online (*Squiggle, Google or CBBC safe search)*
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to

have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

- Be clear about the location, retrieval and evaluation of online knowledge

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites, then the URL will be reported to the *school Online-Safety coordinator.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

8. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- The installation of Impero tracking and monitoring within school for all fixed devices
- The installation in 2016 of Airwatch for Managing iPads.
- The Confide button within Impero for children
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from the Head
- Pupils and staff have to 'accept' an Acceptable Use Agreement (AUA) on screen, once a term, before being allowed access to a computer (see pupil and staff ACUs at the end of this document)
- The filtering provided by KLZ (all State schools in Kent network which we belong to)
- A GDPR compliant change request process for all IT related products/licences

Password Expectations

- 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 4 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.
- For sensitive data being emailed or stored we expect staff to password protect that file.

For more information on data protection in school please refer to our **Privacy policy and Privacy Notice on the website**. More information on protecting personal data can be found in **section 11** of this policy.

9. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by enabling students in Years 4 and above to submit work by email.

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents.

School Email Accounts and Appropriate Use

Children in Y4 and above are allocated a school email account as part of their learning within PSHE. This does not have either their full name or the name of the school and is hosted by KLZ (Kent Learning Zone) once students have completed the module on email safety staff are encouraged to communicate more widely with students by email.

Example email: hansfm02@klz.org.uk

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school-approved email accounts
- Social emailing is not permitted
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Parents should be aware of the following when using email in school.

Email has become the most convenient way to communicate worldwide. The school office will email parents with notifications of trips, reminders of events and school activities. Parents wishing to email staff can do so via the school office or directly to staff. Staff will endeavour to reply as quickly as possible, although this may be the next day.
Please do not assume however that an email will be read before school. Staff are frequently involved in preparation, conversations and meetings or classes before school. Any urgent message for that day should be sent to the office and copied to the form teacher for information.
We would ask parents to send the email to the person who needs to do something and cc for anyone who might need to know or be aware. Always use a title (short is good) in the email to help office staff prioritise. Eg dentist/ lost coat/ homework issue.

Community use of the Internet

Outside organisations wishing to use the ICT facilities will be given a user name with limited permissions. Internet access will be filtered as for a pupil.

10. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. Staff emails are provided for parents to use and guidance around emailing staff is contained in the Parent Handbooks.

The Parent Portal is a password Protected area of the website. This allows communication in a secure environment.

The website is managed by the Director of Admissions and Marketing and her team. Content is provided to her for approval and is uploaded and updated in a timely fashion.

11. Policy on Using Images of Children (see separate policy)

Colour photographs and pupils' work bring our school to life, showcase our students' talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. The Policy on Using Images of Children outlines

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

Parents give consent when the child joins the school**.** This consent is not limited to the time that the child attends the school.

Advice on the Use of Images by parents is given in the Parent Handbooks

Where a pupil has achieved special recognition, news of this, including their name and photograph may be used on the website and in the press. Permission from parents will always be sought.

12 Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's **child protection and safeguarding** policy and **behaviour policy.**

13 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. The laws governing such sites mean that no pupil at the school is of the age where they can legally get such an account. The wifi network blocks access to all social media sites. We do educate pupils for the use of Social networking because we recognise that this happens. Pupils will be advised to use nicknames and avatars when using social networking sites at home. The school does not condone the use of under-age social networking on Snapchat, Facebook, Instagram, What's App etc. by pupils. These sites are blocked on the school network.

As part of our programme to partner with schools abroad students will be participating in live links through Skype or Facetime supervised by staff.

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

14 Radicalisation (PREVENT)

Radicalisation is seen as part of the schools' wider safeguarding Extremist websites fall under the violence category and are blocked across the KPSN (Kent Public Service Network). Any domain that isn't currently in our database falls into the unknown category and is blocked/allowed depending on the status of that category in the relevant rule set. Because of this, the unknown category is blocked for students.

Lightspeed is also in contact with the Home Office and other law enforcement agencies about new websites related to extremism and terrorism so that these can be categorised as promptly as possible.

Advice on Radicalisation has been taken directly from the following sources:

- **DfE – The Prevent Duty June 2015:** https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The School cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the Online-Safety policy is adequate and that its implementation is appropriate and effective.

15. Mobile Phones and Personal Devices

The School cannot accept liability for the material accessed, or any consequences of Internet access of material already contained on a device's memory. Pupils are not allowed nor do they need phones in school. A member of staff can confiscate a mobile phone, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

Pupil iPads, laptops and Kindles registered for use in school to promote inclusion and equality of opportunity may not have 3 or 4G capability and must run over the secure Wifi.

An agreement (BYOD agreement) and policy (BYOD Policy) is in place and signed by pupils and parents outlining the expectations and limitations for their use. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

A list of children with permission to use user owned devices is placed on a centralised spreadsheet which is accessible from the staff area: T:\Whole School\BYOD
Students are also issued with an ID card which is to be kept with the device and to be made readily available when using the device during lessons

Pupil owned mobile phones and iWatches are not permitted in school. This is because mobile devices with wireless Internet access can bypass school filtering systems and other features such pictures and videos can be taken without the person's consent.

A log is kept of Online-Safety concerns dealt with through the school's behaviour system
From September 2016 Online-Safety is a separate behaviour category on SIMS

The school has measures to ensure that mobile phones are used responsibly in school.
Staff are issued with guidance about their use at Induction and all staff sign an Acceptable Use Policy.

16. Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their personal device may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time unless this is a device supplied by the school.

- Staff are permitted to take photos or videos of pupils with iPads provided by the school. In the absence of an iPad on trips off site photos and film can be taken on personal devices providing that photos or video is uploaded onto the shared area and deleted off the device as soon as possible. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.
- Staff are not permitted to use gambling apps or websites at school on any device.

Handling Online-Safety complaints

17.Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying, very seriously**.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

The school's anti-bullying policy will be followed.
If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Repeated bullying may result in exclusion.

18.Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

19.Protecting Personal Data

St Michael's Prep believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress and understands the requirements of the Data protection Act 2018 and GDPR. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. Examination results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 2018, and following principles of good practice when processing data, the school will:

ensure all data is:

- Fairly, lawfully and transparently processed;
- Processed for a specified, explicit and legitimate purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than necessary;
- Secure;

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's Privacy policy and Privacy Notice**

This is available on the school website and on request from the office.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Training and Updates
Training is a regular feature of the School's weekly routine.
The last training on Online-Safety for staff was in May 2018
Training records are held in SIMS.

KCC has a very informative Online-Safety bulletin to which we subscribe (KELSi), which informs our work.
The Head of ICT and Head are trained as CEOP ambassadors and are able to deliver training to pupils and staff using nationally recognised materials.

Working with Parents
We offer annual workshops with external experts to our parents and we also invite the parents of our partner schools to attend. The last training for parents was on 7th Feb 2018

Glossary of terms relating to Online-Safety

Anti-Virus Software	Application designed to protect PC's from malicious computer code (virus)
AUA	Acceptable Use Agreement - set of rules applied to a network, website or computer system that restricts the ways the network site or system may be used.
Avatar	Avatar - A graphic or icon used to represent a person in an online chat-room or game. Avatars can usually be customised and range from simple images to complex three-dimensional shapes.
Backup	The process of copying important computer files and documents from your hard disk to removable media (such as Zip or CD-RW discs) or another computer, to protect against loss of originals.
BitTorrent	A site that enables file sharing, but largely of illegal content
Bluetooth	A wireless technology used to connect devices over short distances so they can share information
Blog	A type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order.
Broadband	Internet connection with high speed rate of transfer

Browse	Using a web browser application to look at websites on the internet
Bullying	Repetitive, intentional, emotional or physical harm, often involving an imbalance of power.
Club Penguin	A virtual world where your avatar can live, meet new people, chat and buy goods.
CEOP	Child Exploitation and Online Protection - dedicated to eradicating the sexual abuse of children. Part of UK policing. Tracks and brings offenders to account. http://www.ceop.gov.uk
Console	A term often used for a computer built for a specific purpose such as playing games. Examples include PlayStation, Wii, Xbox and DS.
Content Control	Software designed and optimized for controlling what content is permitted to a reader, can be used to restrict material delivered over the Web.
Cyber Bullying	When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass or harm another person. (expanded definition below)
Download	Process of transferring files onto your PC directly from another computer. You might, for instance, download pictures, a movie or a file from the internet.
Email	A means of sending a message electronically over a long distance where there can be benefit in coping with a delay in transmission or receipt.
Encryption	The science of scrambling data be it text, audio, or video so that it can only be read by the authorised sender and recipient.
File Sharing	File sharing is the practice of distributing or providing access to digitally stored information, such as computer programs, multi-media (audio, video), documents, or electronic books.
Firewall	A system that prevents unauthorised access to a computer over a network, such as the internet. Firewalls can be either hardware or software businesses tend to use the former; home users the latter.
Filtering	Software or hardware product designed to prevent access to inappropriate websites on the internet. It does this by denying or allowing access based on lists of pre-classified addresses, or by examining the web data for keywords or unwanted content.
Hacking	Slang term used to describe illegal access of computer systems by unauthorised users.
Happy Slapping	Taking and publishing pictures of assault online.
Identity Theft	Stealing and then using someone else's personal details for immoral gain.
IM	Instant Messaging - a form of real-time communication between two or more people based on typed text. The text is conveyed via devices connected over a network such as the internet. Main examples are BBM (Blackberry Messenger) and MSN (Microsoft Network). Can also be used to share files.
iStock	Internet based service who buy and sell royalty-free photographs, vector illustrations, video footage, audio tracks and flash files.
Google	A search engine, but used as the generic term for searching online.
Grooming	The process of manipulative persuasion for immoral gain; can involve aggressive tactics like blackmail or financial incentives. Adults befriend, flatter and trap young people into doing what they say (often sexual) usually by threatening them once they have an image that could be misused.
Netiquette	A term referring to good behaviour while connected to the Internet. Netiquette mainly refers to behaviour while using Internet facilities such as individual Web sites, emails, newsgroups, message boards, chat rooms or Web communities.

Ofcom	Is the communications regulator. They regulate the TV and radio sectors, fixed line telecoms and mobiles, plus the airwaves over which wireless devices operate. http://www.ofcom.org.uk
PC	A personal computer.
Patching	Software file or collection of files that fixes problems with existing applications by making changes to the program.
Phishing	The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
Pharming	The process of collecting information from a computer by hidden means - often makes use of computer programs called spyware.
Preferences	Part of a program that lets you alter various settings and remembers changes so it looks and behaves how you want.
PSHE	Personal, Social and Health Education
Sexting	The sending of explicit pictures (often self-portraits) by multimedia text.
Sign up	Accept terms and conditions of use, copyright, IPR and liability and usually give up some personal information in return for a service.
Spam	Junk email sent to large groups of people offering money-spinning ideas, holidays, virus ridden payloads and so on. Named after the Monty Python Spam song.
Spit and Spim	Like spam, but sent via instant messaging (SPIM) or VOIP (SPIT)
Social Networking	A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services. Examples include Bebo, Facebook, and Myspace.
Triple X content	.xxx - a domain which is reserved for the online pornography industry. Also used to refer to websites which contain adult content.
Trojan	A computer program that takes control of the computer it is installed upon without the knowledge of the owner.
Tweets	Tweets are text-based posts on the social networking site Twitter. They are displayed on the author's profile page and delivered to the author's subscribers known as followers. Can be restricted to a circle of friends or, by default, allow open access.
Upload	Process of transferring information to another computer, often for publishing on the internet as a web page. The process normally involves using FTP (File Transfer Protocol).
USB	Universal Serial Bus - A standard allowing quick and easy connection of a wide range of peripherals including memory sticks, scanners and printers to your PC. It supports 'Plug and Play' and devices can be added or removed with the PC switched on.
VLE	Virtual Learning Environment - Programs to support teaching and learning. One type of VLE is Moodle.
VoIP	Voice over Internet Protocol - Technologies to used to transmit voice over the internet or other networks (internet telephony)
Web Cam	A video camera designed to connect to your PC. It can be used to record video clips and still images which you can send by email, uploaded or transmitted directly over the internet for video-conferencing.
White Listing	A list or register of things that, for one reason or another, provide a particular privilege, service, mobility, access or recognition.

Wi Fi	Known as wireless broadband, wireless networking or wireless fidelity. Simply means broadband without wires.
World of Warcraft	A virtual world, where your Avatar can live, meet new people, chat, buy goods, develop characteristics and power over peers

Online-Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the Online-Safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an Online-Safety Policy that complies with current guidance?	Yes
Date of latest update: *January 2017*	
The Policy is available for staff on the school Network in Whole School/ Policies	Yes
And for parents on the website	Yes
The Designated Safeguarding Lead (DSL) is: *Gordon Baird*	
The Online-Safety Coordinators are: *Jamie Booth and Jo Salmon*	
Has Online-Safety training been provided for both students and staff?	Yes JBO 20.9.2016
Do parents sign and return an agreement that their child will comply with the School Online-Safety Rules?	Yes

Have school Online-Safety Rules been set for students?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access (e.g. KLZ).	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

Online-Safety Audit

The Online-Safety audit is via the Online-Safety Evaluation Tool which can be located in **Annex F.** This document will help the Head of ICT and Computing and senior leadership team (SLT) assess whether the Online-Safety basics are in place to support a range of activities.

Signed by

_____ **Chair of governors** **Date: .....**

_____ **Headteacher** **Date: .....**

This policy will be reviewed every three years or when KCSIE changes.

Appendices to be added to this policy

1. Overview of Online-Safety teaching 2016-17
2. Consent form for pupils 2016-17

Policies and documents that relate to this policy

Safeguarding and Child Protection Policy
St Michael's Acceptable Use of ICT, Mobile Phones and Social Networking
Acceptable Use of ICT Agreement
BYOD (Bring Your Own Device) Policy and Agreement
Anti-Bullying Policy
Data Protection Policy
Behaviour and Reward Policy

Useful links
http://www.kelsi.org.uk/pru,-inclusion-and-attendance/pupil-referral-unit/Online-Safety-classroom-materials

http://www.kscb.org.uk/

Annex A

Self-Evaluation Tool for Schools Online Safety Practice

Policies and practice	No	Partly	Yes	Comments/Actions /Evaluation
Is online safety clearly identified as a safeguarding issue within the school with appropriate Senior Leadership Team (SLT) strategic oversight to ensure that leaders oversee the safe use of technology and can take action immediately if they are concerned about bullying or children's well-being?				
Is the SLT aware of the statutory responsibilities regarding safeguarding which includes online safety? For example, Keeping Children Safe in Education (2015) and the Prevent Duty.				
How are SLT engaged and involved with ensuring the online safety agenda is shared and communicated with stakeholders?				
Does the school have a set of robust online safety policies and practices which cover the following issues: use of mobile phones/personal devices, use of images/cameras, social media, education/training for children and staff?				
Is the online safety policy specific to the schools needs and requirements e.g. taking into account technology access and needs/requirements of pupils?				
When was the online safety policy last updated? (N.B. this is recommended to be reviewed annually)				
How were stakeholders involved in creating or reviewing the policy e.g. staff, parents/carers, children?				
Is the online safety policy cross referenced with other appropriate school policies e.g. anti-bullying policy, behaviour, searching, data security and safeguarding etc?				
How is the operation of the schools policies checked and enforced by the school?				
Have the policies been approved by the Governing Body? If so, when?				
Is the policy clearly communicated with the wider school community e.g. is the online safety policy available on the school website?				
Does the school have a robust acceptable use policy (AUP) which is appropriate for all members of the community? If so, when was it last updated? (N.B. schools may have multiple AUPs for different audiences)				
How does the school ensure that the AUP is understood and respected by pupils, staff and parents?				
Are there clear reporting mechanisms in place for online safety concerns for staff, pupils and parents/carers? If so, what are they? E.g. flowcharts, reporting buttons/emails etc and are specific members of staff identified as points of contact?				
Are there effective sanctions in place for breaching the school's online safety policy or AUP? If so, what are they and where are they located (e.g. in the behaviour policy)?				

Does the school have an online safety Coordinator/lead (or group) with clearly defined responsibilities? If so, who are they? (NB recommended Designated Safeguarding Lead (DSL) and/or SLT)				
Does the school keep an online safety incident log?				
How is the incident logged used to inform and review practice?				
Is there a member of the Governing Body with responsibility for online safety? If so, who and have they received appropriate training?				
Does the school understand the impact level of personal data and is data managed securely and in accordance with the statutory requirements of the Data Protection Act 1998 e.g. written consent to take/share images, school provided email addresses used, school provided devices, strong passwords, encryption of personal information and use of secure email?				
Infrastructure	**No**	**Partly**	**Yes**	**Comments/ Actions / Evaluation**
Is the schools network safe and secure? E.g. devices which leave the site are encrypted, strong passwords are in place (for all but the very youngest users) and screen locks are enforced.				
Does the school use an accredited/education appropriate internet service provider and relevant filtering/monitoring products?				
How does the school monitor the school network and internet use for safeguarding or security concerns? E.g. key word monitoring, history checks etc.				
How are filtering decisions made by the school?				
How does the school manage and respond to filtering/security breaches?				
What devices does the school have e.g. tablets, laptops etc and how has the school ensured that these devices are used safely and that education, policy and procedures have been updated to reflect school technology use?				
Education and Training	**No**	**Partly**	**Yes**	**Comments/Actions / Evaluation**
Do **all** members of staff (including all support staff) receive regular, appropriate and up-to-date online safety training and guidance which enables them to understand how the internet/technology can be used to groom, radicalise or abuse pupils?				
How is online training delivered to all staff? How does the school ensure that this training is up-to-date?				
Has the DSL or at least one member of senior leadership staff attended appropriate training to ensure they have a higher level of expertise and understanding of online safety issues?				
How does the school ensure that all members of staff understand the school policies and procedures regarding online safety?				

Do all members of staff know how to protect their online reputation understand the expectations and boundaries regarding safe and appropriate relationships and communications with pupils/parent via social media? e.g. staff do not share any personal information with pupils/parents and all communication takes place within clear and explicit professional boundaries which are transparent and open to scrutiny?				
Do all children receive a progressive and embedded online safety education? • Is the online safety education within the school progressive and embedded throughout the curriculum for all ages? E.g. www.digital-literacy.org.uk • How are special or specific events used to support this? • Are peer mentoring programmes/schemes used?				
How does the school ensure that there are strategies in place to help keep pupils safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe?				
How does the school ensure that vulnerable pupils access appropriate education relating to online safety e.g. targeted or differentiated support/resources?				
Is the school able to demonstrate internal capacity for online safety awareness and education? (E.g. external speakers are used to compliment student education and are not used in isolation).				
Does the school participate in local and national events such as Safer Internet Day?				
Does the school reward positive use of technology? If so, how?				
How does the school work to help and support parents/carers understand Online safety issues and risks and their roles and responsibilities at both home and school? How has this been communicated and developed e.g. workshops, newsletters, online safety area on school website etc.?				
Does the school have online safety information for staff, pupils and parents on the school website e.g. school policies and contacts, CEOP button, links to ThinkUKnow, IWF, Childnet and UK Safer Internet Centre?				
Does the school use social networking/media as a form of communication? If so has this been risk assessed and approved by SLT and are appropriate safety measures been taken?				
Is Online safety covered as part of the home school agreement?				
Standards and inspection	**No**	**Partly**	**Yes**	**Comments/Actions / Evaluation**
Has the school conducted an audit of the current online safety and safeguarding measures? E.g. 360 safe: www.360safe.org.uk				

Does the school complete appropriate risk assessments regarding use of technology?			
How does the school monitor and review measures and practice after dealing with incidents/concerns?			
How does the school monitor, review and evaluate all of the above?			
Any other points or comments			

Next Steps

Key area for development	Justification	Action & Resources / support needed	Lead Staff & time allocation

Annex B

Year Group	Online-Safety Topic/s covered:
Year 1	What do we use computers for? What is the difference between the computers and iPads? What do you enjoy doing on the computer? What is a link? What is an advertisement?
Year 2	What do you enjoy doing on a computer or iPads? Is it different at home and school? Why? What do we do if we see something that makes us feel uncomfortable? Recap on Computer use and Internet Safety Rules Reporting and Blocking
Year 3	Can you just take any picture and use it? Should you give your real name online? Real address? What situations would people ask you for your real name? Can you trust all the information you see / find out on the internet? When do you prefer to use an iPad or a computer? Music online and the law.
Year 4	Email safety, netiquette, chain mails, attachments, viruses, Trojans etc How would you respond to online bullying? The differences between face to face and online bullying. What would you do with a text message you don't like or that makes you feel uncomfortable? How do you use blogs? What sort of comments should you leave? What do you do if someone leaves a comment that makes you feel bad? How can you find the author of a document or website?

Year 5	When do you meet people online? When do you give your real name? Would you create a whole new online persona? Why would people not keep their real name online? Why do some websites have age restrictions? Is it wrong to break the rules to be a member? Research skills, evaluating websites, retrieval, reliability of information and acknowledging sources Films online and the law File sharing
Year 6	What does it mean to lie about your age for sites such as Facebook or Snapchat? Problems with chatrooms Staying safe when using chatrooms Introduction to concept of bad people online and grooming How do you respond to blog posts? What happens if someone leaves a comment that makes you feel bad? What should you do? Think before you post. Online gaming
Year 7	Cyber Bullying, through texts, chatrooms, IM websites, social media, what's app, Instagram, using videos, manipulating images and text, sharing, posting on YouTube Potential risks to their safety and wellbeing and steps to reduce these risks. How a young person can be tricked by someone pretending to be a friend of a similar age Staying safe whilst chatting online. Rules for chatrooms Blogging
Year 8	Social Media / What is it? Dangers of using Social Media What students should and should not do when using Social Media Phishing Sexting The law on Sexting Grooming for Sexual exploitation or radicalisation Pornography