

St Mark's CE Primary School

Ramslye Road
Tunbridge Wells
TN4 8LN



Online Safety Policy

Headteacher: Robin Dungate
Chair of Governors: David Hill

Ratified: 10th October 2016 at the FGB
Review date: October 2017

Signed by Chair of Governors

Date

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

St Mark's CEP School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

St Mark's CEP School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

St Mark's CEP School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions. St Mark's CEP School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of St Mark's CEP School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that St Mark's CEP School is a safe and secure environment.
- Safeguard and protect all members of St Mark's CEP School community online.
- Raise awareness with all members of St Mark's CEP School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

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

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Sex and Relationships Education (SRE), Code of Conduct for ICT.

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Leads (DSL) is R DUNGATE and S BIRD

The Online safety (e-Safety) lead for the Governing Body is G Douglas

Policy approved by Head Teacher/Manager: R Dungate Date: October 2016

Policy approved by Governing Body: D Hill (Chair of Governors) Date: 10/10/16

The date for the next policy review is October 2017

St Mark's CEP School online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.

The policy has been approved and agreed by the Leadership/Management Team and Governing Body. The school has appointed the Designated Safeguarding Leads R Dungate and S Bird as appropriate members of the leadership team and the online safety leads. The school has appointed G Douglas as the member of the Governing Body to take lead responsibility for online safety (e-Safety).

The online safety (e-Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

1.3 Key responsibilities for the community

Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.

Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.

Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.

Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including a Code of Conduct for ICT which covers appropriate professional conduct and use of technology.

To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.

To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.

Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.

Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.

Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.

Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.

Keeping up-to-date with current research, legislation and trends regarding online safety.

Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.

Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms

Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need

To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.

Liaising with the local authority and other local and national bodies, as appropriate.

Working with the school/setting leadership and management to review and update the online safety policies and other related policies on a regular basis (at least annually) with stakeholder input.

Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

Contributing to the development of online safety policies.

Reading the school Code of Conduct for ICT and adhering to it.

Taking responsibility for the security of school/setting systems and data.

Having an awareness of a range of different online safety issues and how they may relate to the children in their care.

Modelling good practice when using new and emerging technologies

Embedding online safety education in curriculum delivery wherever possible.

Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.

Knowing when and how to escalate online safety issues, internally and externally.

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.

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

Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.

Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.

Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

1.3.5 The key responsibilities of children and young people are:

Contributing to the development of online safety policies.

Reading the school/setting Code of Conduct for ICT and adhering to it.

Respecting the feelings and rights of others both on and offline.

Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

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

Taking responsibility for keeping themselves and others safe online.

Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

Reading the school/setting Code of Conduct for ICT, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

Role modelling safe and appropriate uses of technology and social media.

Identifying changes in behaviour that could indicate that their child is at risk of harm online.

Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).

(The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.)

The head teacher/manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright..

2.2 Publishing images and videos online

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

The school/setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Code of Conduct for ICT, Image Use.

In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

Pupils may only use school/setting provided email accounts for educational purposes

All members of staff are provided with a specific school/setting email address to use for any official communication.

The use of personal email addresses by staff for any official school/setting business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.

Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.

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

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.

The school/setting's internet access will be designed to enhance and extend education.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability

- At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school owned devices will be used in accordance with the school Code of Conduct for ICT and with appropriate safety and security measure in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.

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

When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

3. Social Media Policy

3.1. General social media use

Expectations regarding safe and responsible use of social media will apply to all members of St Mark's CEP School community and exist in order to safeguard both the school/setting and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

All members of St Mark's CEP community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

Information about safe and responsible use of social media will be communicated clearly and regularly to all members of St Mark's CEP community.

All members of St Mark's CEP community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The school/setting will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems

The use of social networking applications during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.

Any concerns regarding the online conduct of any member of St Mark's CEP community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

St Mark's CEPS does not have any official social media channels

3.3 Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school/setting

All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels

Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.

Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.

Members of staff will be encouraged to manage and control the content they share and post online.

Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

Members of staff are encouraged not to identify themselves as employees of St Mark's CEPS on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and also to safeguard the privacy of staff members and the wider community.

Members of staff will ensure that they do not represent their personal views as that of the school/setting on social media.

School/setting email addresses will not be used for setting up personal social media accounts.

3.4 Staff official use of social media

St Mark's CEPS does not have any official social media channels

3.5 Pupils use of social media

St Mark's CEPS does not have any official social media channels.

A leaflet for parents entitled 'Children's ICT and e-safety' is available on the school website.

Safe and responsible use of social media sites will be outlined for children and their parents.

Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

Any official social media activity involving pupils will be moderated by the school where possible.

The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.

Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of St Mark's CEP School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by children during school hours is prohibited.

St Mark's CEP School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

The use of mobile phones and other personal devices by children during school hours is prohibited. All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school/setting accepts no responsibility for the loss, theft or damage of such items. Nor will the school/setting accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Mobile phones and personal devices are not permitted to be used in certain areas within the school/setting site such as changing rooms, toilets and swimming pools.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.

Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.

All members of St Mark's CEP School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of St Mark's CEP School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.

Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

4.3 Pupils use of personal devices and mobile phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.

Pupil's personal mobile phones and personal devices will be kept in a secure place in the office, switched during school hours.

4.4 Staff use of personal devices and mobile phones

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Code of Conduct ICT

4.5 Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school Code of Conduct for ICT

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

St Mark's CEP School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. This is monitored by PJA Systems. We also receive reports from e-safe for any inappropriate online searches

The school will take all reasonable precautions to ensure that users access only appropriate material.

However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.

The school will audit technology use to establish if the online safety (e-Safety) policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.

5.2. Internet use throughout the wider school/setting community

The school will liaise with local organisations to establish a common approach to online safety.

The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.

5.3 Authorising internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.

All staff, pupils and visitors will read and sign the Code of Conduct for ICT before using any school resources.

Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.

All users will be informed that network and Internet use will be monitored.

Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.

6.2 Engagement and education of children and young people considered to be vulnerable

St Mark's CEP School is aware that some children may be considered to be more vulnerable online due to a range of factors.

St Mark's CEP School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.

Staff will be made aware that our Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential when using school systems and devices.

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

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

St Mark's CEP School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

7. Managing Information Systems

7.1 Managing personal data online

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

Full information regarding the schools approach to data protection and information governance can be found in the schools information security policy.

7.2 Security and Management of Information Systems

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

Password policy

- All users will be informed not to share passwords with others and not to login as another user.
- 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.
- We require staff and pupils to use STRONG passwords for access into our system.

7.3 Filtering and Monitoring

The governors/proprietors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.

The filtering system in place is supplied by the local LEA and is monitored by PJA Systems Ltd.

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

All monitoring of school systems will take place to safeguard members of the community.

All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.

Any inappropriate sites that pupils or teachers find should be reported to both teams. We also receive reports from e-safe for any inappropriate online searches

If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.

The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

All changes to the school filtering policy will be logged and recorded.

The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

The headteacher/manager is ultimately responsible for the security of any data or images held of children.

Apps/systems which store personal data will be risk assessed prior to use.

Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.

Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure

Any complaint about staff misuse will be referred to the head teacher

Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Pupils, parents and staff will be informed of the schools complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school/setting community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.

Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or “Sexting”

St Mark’s CEPS ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as “sexting”).

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

St Mark’s CEPS views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead .

The school will follow the guidance as set out in the non-statutory UKCCIS advice ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ and KSCB “Responding to youth produced sexual imagery” guidance

If the school are made aware of incident involving creating youth produced sexual imagery the school will:

The school will not view an images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).

The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.

The school will take action regarding creating youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

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

St Mark’s CEPS will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

St Mark’s CEPS views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the Safeguarding Team by the DSL.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
 - Immediately notify the designated safeguarding lead.
 - Store any devices involved securely.
 - Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
 - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Make a referral to children's social care (if needed/appropriate).
 - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
 - Inform parents/carers about the incident and how it is being managed.
 - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
 - The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
 - If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
 - The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

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

St Mark's CEPS will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.

If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

- Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.

Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

9.5. Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of St Mark's CEPS community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

9.6. Responding to concerns regarding online hate

Online hate at St Mark's CEPS will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour

All incidents of online hate reported to the school will be recorded.

All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.

The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Appendix E

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:

www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e-Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/online-safety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: <https://360safe.org.uk/>

Online Compass (Self review tool for other settings): <http://www.onlinecompass.org.uk/>

