St Margaret's Preparatory School

Online Safety Policy

Date Policy Reviewed	Policy Reviewed By	Reason/Outcome	Next Review Due
September 2016	Simon Clinch and Carolyn Moss	Review	Sept 2017

Our Vision

- We want… every child to love coming to school and to love learning.
- We want… all children to feel secure and cared for.
- We believe… in teaching the whole child and finding exciting ways to enhance their learning experience so that when they leave St. Margaret's, they say what a fantastic school it is in every way.

And this is what we aim to do

- Provide a high quality education, where children can grow in knowledge and understanding.
- Equip all children with appropriate skills, attitudes and values.
- Create an environment where every child can fulfil their potential.
- Encourage every child to benefit from our caring staff and fine facilities.
- Enable every child to communicate with confidence in every situation.
- Treat every child with the highest standards of courtesy, loyalty, honesty and fairness, and expect the same from them in return.

Purpose of the Policy

St Margaret's Preparatory School 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 practice good e-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.

E-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. 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 e-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. E-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.

1. Roles and responsibility

The School e-Safety Officers are Mrs C Moss (Designated Safeguarding Lead) and Mr S Clinch (ICT Coordinator). Both have completed the NSPCC *Keeping Children Safe Online* course and are responsible for arranging yearly staff INSET. A yearly Self Assessment form will be undertaken to ensure e-Safety needs are being met throughout the school (see Appendix 1).

2. 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 e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons and assemblies where personal safety, responsibility, and/or development are being discussed. Parent meetings and training is also available on an annual basis.

3. What is an e-Safety Incident?

Given the enormous complexities of the factors that may constitute 'risk', the following grid is helpful in providing some structure by providing a classification system of categories linked to boundaries:

The grid below (developed by the EUKids Online project. Hasenbrink, Livingstone, Haddon, Kirwil and Ponte, 2007) provides some structure to the potentially broad ranging set of factors that constitute 'risk' in this area. It is important to remember that there is overlap between some of these categories and boundaries are sometimes blurred. In using these three categories on Content, Contact and Conduct, it is possible to contextualise a definition of 'potentially harmful or inappropriate material'. It is acknowledged that in practice there may be overlap between categories and that boundaries are frequently blurred, but it may also provide a useful framework for 'replacing emotion with facts' when confronted with specific issues or concerns. It is also helpful to exemplify the broad range of potentially harmful or inappropriate behaviours, in terms of raising awareness and educating key audiences.

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent / hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info / advice

4. 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.

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

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- 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.
- Use of iPads in Early Years and Laptops in Pre-Prep and Prep lessons.
- Junior Librarian System integrated with cloud technology, allowing children access to a controlled VLE and resource bank.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- To track pupil's progress throughout the year.

For parents:

- To liaise with parents via ParentMail, email and Padlets.
- To give parents access to the Parent Area of the website to keep updated on current information.

5. 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
- to use age-appropriate tools to search for information online
- to 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.

The school filters 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 e-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.

6. 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 security of the school information systems and users will be reviewed regularly by the ICT Technician, under the guidance of Cognita, and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers
- 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 a member of the senior management team.

For more information on data protection in school please refer to our **data protection policy**.

7. Emails

The school uses email internally for staff, and externally for contacting parents, and is an essential part of school communication. If an external email is to be sent to a parent then staff should be aware that they are representing the school and that factual information should be communicated in a professional manner.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact other members of staff and other professionals for work purposes; this is important for confidentiality. The school and Cognita has the right to monitor emails and their contents but will only do so if it feels there is reason to.

7.1 School email accounts and appropriate use

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

- 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 the ICT Coordinator or a member of the 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.

Pupils will be educated through the Computer Science / 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.

8. 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. No personal information on staff or pupils will be published in the public domain and details for contacting the school will be for the school office only. Children's full names will not be published on the website.

The website will be maintained by designated staff only, currently those with administrator access within school are:

Mrs J Last	Registrar
Ms E Cosby	Cognita Head Office
Ms S Hunt	Cognita Head Office

8.1 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our student's 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.

Parents are reminded regularly to not upload any photographs taken inside the school to Social Media (see paragraph 8.4).

8.2 Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only and must not be published on any social media sites.

- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our **school child protection and safeguarding policy.**

8.3 Complaints of misuse of photographs or video

Parents should follow the 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 schools **child protection and safeguarding** policy and **behaviour policy.**

8.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms, online gaming and instant messaging programs. 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 students 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. There are various restrictions on the use of these sites in school that apply to both students and staff.

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 PSHE 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 the LT and will be moderated by a member of staff.
- Pupils and staff will not 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.

9. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school.

- The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy.**
- Students are not permitted to bring Mobile Phones into the school, unless an agreement with the school is already in place. In this instance, the device should be taken straight to the school office for safe keeping until the end of the day.
- Staff Mobile phones must be switched off or placed in silent mode during school lessons or any other formal school activities.
- Pupils are not permitted to bring mobile devices into the school.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.
- Staff teaching Early Years must ensure their phones are switched off and locked away when teaching.

8.2 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 mobile phone will be confiscated.

Staff

- Staff are not permitted to take photos or videos of pupils. 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' whilst on duty – this includes any formal events outside of 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.

10. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the **behaviour, anti-bullying and cyberbullying policies.** 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.

If an allegation of bullying arises, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.
- contact CEOPS, via the Safeguarding Officer in cases of child protection.

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.

In addition to this, parents should be aware that cyberbullying legislation also applies to their use of social media and other communications. Evidence of cyberbullying of a member of staff will be taken very seriously by the School.

11. 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.

12. Protecting personal data

St Margaret's Preparatory School 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. 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. Assessment 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 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

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 data protection policy.**

13. Procedures to Follow

Should staff, pupils or parents be concerned about e-Safety then they must talk to the designated person:

- Staff should discuss concerns with the e-Safety or Designated Safeguarding Lead (or Deputy);
- Parents are encouraged to contact the school;
- Pupils are encouraged to talk to a 'responsible adult' – be that their Parent or Teacher.

Parents, children and staff all have access to Childline and CEOP via the school website and are informed how to use these agencies.

If an e-Safety incident occurs, the e-Safety officer will complete an 'Incident Log' (Appendix 2) with the person(s) who raised the concern. With this information they will then discuss the issue with the relevant person, be that the Headmaster or the Designated Safeguarding Lead, depending on the severity of the incident.

Should the issue need escalating further, then CEOP and the Police will be contacted by the Child Protection Officer (see the school Safeguarding Policy for guidance in reporting incidents).

14. British Values

Pupils are taught

- To appreciate viewpoints of others on ethical issues
- To engage in an online community positively, responding appropriately to others and leaving a positive digital footprint
- How to be respectful digital citizens
- Acceptance of British Values of democracy, ensuring all student's work and views are appreciated
- How to select information from valid online sources that reflect different viewpoints and the disadvantages of relying on Wikipedia
- The value of blogs to understand different viewpoints on a range of topics contribute positively to life in modern Britain
- The dangers of the internet are highlighted to students and they are taught about what to do if they are uncomfortable with any online behaviour or material.

15. Anti-radicalisation

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school block inappropriate content, including extremist content.

- Searches and web addresses are monitored by teachers and the ICT technician, who will alert the Leadership Team where there are concerns.
- The ICT technician will block access if extremist sites are found.
- Staff, pupils and visitors must report unblocked extremist content to a senior member of staff.

Appendix 1

Self Assessment Form

Appendix 2

e-Safety Incident Log