17 49

ST MARGARET'S

SCHOOL

E-Safety Policy
Including EYFS

Reviewed and updated September 2022

Introduction

It is the duty of St Margaret's School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social media platforms;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

See further information on 'new generation' technology, social networking and e-mail at **Appendix 1 – 3**.

This policy, supported by the Pupil Acceptable Use agreements below (see **Appendix 4** and **Appendix 5**), is written in line with *Keeping Children Safe in Education 2022 ("***KCSIE 2022***")*, *Teaching Online Safety in Schools 2019* and statutory guidance. KCSIE 2022 sets out specific responsibilities for governing bodies to ensure:

- pupils are taught about online safety
- appropriate filters and appropriate monitoring systems are in place, and
- online safety training for staff is integrated as part of the overarching safeguarding approach.

This Policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection and Safeguarding
- Staff Code of Conduct;
- Health and Safety;

- Behaviour;
- Anti-Bullying;
- Acceptable Use agreement (See **Appendix 4** (Junior School) and **Appendix 5 (**Senior School);
- Data Protection;
- Bring Your Own Device; and
- PSHE.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Margaret's School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the School community, including staff, pupils, parents and visitors, who have access to and are users of the School's IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

Both this policy and the Acceptable agreements cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

1. The Governing Body

   The governing body of the School is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.
   Rachel Hodgson, the Safeguarding Governor will liaise with the School in relation to e-safety.

2. Headteacher and the Senior Leadership Team

   The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has delegated day-to-day responsibility to Mr A. Pirouze (IT Manager) and the e-safety coordinator, Miss J. Chatkiewicz (Vice Principal).

   In particular, the role of the Headteacher and the Senior Leadership team is to ensure that:

a. staff, in particular the e-safety coordinator are adequately trained about e-safety; and
b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the School.

3. E-safety coordinator

   The School's e-safety Officer, Alexia Winslett is responsible to the Headteacher for the day to day issues relating to e-safety. The e-safety coordinator has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. IT staff

   The School's technical staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the School's hardware system, its data and for training the School's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the e-safety coordinator.

   Contact Person: Mr A. Pirouze – IT Manager

5. Teaching and support staff

   All staff are required to sign the Staff Acceptable Use Policy before accessing the School's systems. The Staff Acceptable Use Policy can be found in the Staff Handbook.

   As with all issues of safety at this School, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

6. Pupils

   Pupils are responsible for using the school IT systems in accordance with the Pupil Acceptable Use agreements (see **below**), and for letting staff know if they see IT systems being misused.

7. Parents and carers

   St Margaret’s School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and

risks related to internet usage. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

Parents and carers are responsible for endorsing the School's Pupil Acceptable Use agreements.

Education and training

1. Staff: awareness and training

   New staff receive information on St Margaret's e-Safety and Acceptable Use policies/agreements as part of their induction.

   All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of pupils within the context of e-safety.

   All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

   Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

   A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the School's e-Safety Coordinator and Safeguarding Lead.

2. Pupils: e-Safety in the curriculum

   IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

   The School provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons.Students will also participate in the Online Safety Alliance Certificate course in February. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

   At age-appropriate levels, and usually via PSHE, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year 7, pupils are taught about recognising the risks of online sexual exploitation, stalking and grooming, and of their duty to report any such instances they or their peers come across. Pupils can

report concerns to the Safeguarding Lead, their Head of Year, Head of Section and any member of staff at the School.

From year 8 pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities. Staff are aware that when setting a research task that utilises online resources, a list should be provided to ensure that pupils are only accessing the required information

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach the Safeguarding Lead School Counsellor, e-Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents will receive a half-termly letter for parents providing advice about how to support their children as they navigate the online world. The letter will also draw their attention to any safeguarding warnings concerning apps and social media.

The School recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The School therefore arranges discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their child without curbing their natural enthusiasm and curiosity.

For further information on ‘new generation’ technology, social networking and e-mail, please refer to **Appendix 1 – 3**.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the BYOD Policy in the Staff Handbook for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at St Margaret's School are permitted to bring in personal devices for their own use. EYFS - Staff are not permitted to use their personal mobile phone devices or cameras in school. Staff who wish to use their personal mobile devices or cameras in school for any reason must do so in an office or staff room. Staff who act in breach of this may be subject to disciplinary action. Parents are not permitted to use their mobile phones or cameras in or around the EYFS setting unless at an assembly or special performance with the permission of the school.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under any circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, and will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The School has introduced the use of pupil owned electronic devices as a teaching and learning tool and pupils are required to adhere to the Pupil BYOD Policy when using such devices for schoolwork. In particular, the Pupil BYOD Policy requires pupils to ensure that their use of electronic devices for schoolwork complies with this policy and the Acceptable Use agreements and prohibits pupils from using electronic devices for non-school related activities during the school day.

The School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the pupil's Head of Year to agree how the School can appropriately support such use. The Head of Year will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

For information on the use of email, internet and communications systems, please refer to the Staff Handbook.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork purposes, pupils should contact the IT Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the e-Safety Coordinator, IT Manager or another member of staff.

The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Coordinator, IT Manager or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour Policy. Pupils should be aware that all internet usage via the School's systems and its wifi network is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the IT Manager for assistance.

3. Data storage and processing

The School takes its compliance with the UK General Data Protection Regulation and the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their or to the School's central server / Google Drive Account as per the IT Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The School expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

The School will at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates. The School will also complete a data protection impact assessment and check the terms and conditions of sites/apps used for learning purposes (where necessary) to ensure that personal data is being held securely.

The School will destroy or delete data securely and in line with the School's [Data Retention] Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the e-Safety Coordinator or Data Protection Lead.

4. Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy / IT Policy / EYFS Policy / the Child Protection Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such

images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

St Margaret's School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the School's policies and procedures (in particular the Child Protection and Safeguarding Policy).

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Complaints

As with all issues of safety at St Margaret's School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Coordinator in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using MyConcern and reported to the School's E-Safety Coordinator and the Designated Safeguarding Lead, Miss J Chatkiewicz, in accordance with the School's Safeguarding Policy and to the E-Safety Officer Mrs Alexia Winslett

APPENDIX 1

Advice for parents regarding 'new generation' technology and e-safety

Teenagers today have greater expertise and freedom to explore the world of the internet and experience all the fantastic opportunities that the 'virtual world' affords. However, as in the real world, there are risks attached.

At St Margaret's School, we have a rolling programme of information and education on cyber-technology and its use on e-safety. This has been devised to inform and educate, in order for all our young people to make informed decisions, assess the risks and keep themselves safe. This is as important on the internet as out and about on the street.

Our filtered network and screen monitoring have enabled us to supervise and safeguard school computer users, and will continue to do so for all who use personally owned laptops and other devices connected to the school networks. However, the recent increased ownership and use of laptop computers with built-in webcams and live video facilities such as Skype and Facetime, and 'internet enabled' devices which do not need a connection to the school network, such as 3G/4G/5G phones, means that young people are more vulnerable, since these devices have unfiltered and unsupervised connection to the internet.

There are implications for both day pupils and boarders, and their families.

At home, families can keep computers in supervised areas. However, with the new technology, it is easier for young people to go online anywhere, at any time.

In the boarding house here at school, many of the pupils have these 'new generation' devices. We will continue to educate and encourage good sense, and house staff will be aware of the presence of the devices and that they might be used in study bedrooms. Although we will supervise discreetly, you will understand that we cannot guarantee that inappropriate use is not being made of such communications devices.

Communication takes place with parents advising them about e-Safety, and information sessions are arranged on a regular basis to keep them up-to-date with developments in technology.

Owners of new technology devices must therefore take responsibility for their use. We will continue to educate and advise, and ask parents to work with us in this endeavour to enable your sons and daughters to enjoy and benefit from the technology safely.

APPENDIX 2

Social Networking

Social networking and the use of chatrooms is ubiquitous in teenage (and younger) circles and part of adolescent culture. St Margaret's School has decided to manage this development both by restricting access and by educating pupils on the safe use of such websites.

We insist upon the proper and educational use of the school network. The ICT Approved Use Policy proscribes the use of chatrooms and proxy sites. Social networking sites are not to be used during lesson times, or not at all by those under the age of 13.

Monitoring will be active. In the first instance, members of staff are to remain alert to the possibility and ask any pupil observed to have an inappropriate site open during the school day to close it immediately. They should then report the pupil to the Vice Principal.

In addition, all screen content and keyboard activity is automatically monitored by the school system's software. Whenever a violation is triggered, or an attempt is made to access a forbidden file or URL, the screen is automatically captured and maintained within a secure database. This creates a comprehensive audit log, incorporating images and violation details that provides evidence which is reviewed regularly by a member of the Senior Management Team.

APPENDIX 3

E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsibly online.

Managing e-mail

- The School gives all staff and governors their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Staff and governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The School email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- The School requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the School'.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- When emailing pupils across the School, including Sixth Form, another member of staff should always be copied into the communication. We would suggest that this is either the pupil's Head of Year or the Form Tutor. This also includes invitations to Google Meets.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your school job may be disclosable under data protection law. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
    - Review the School's Data Protection Policy and [Data Retention] Policy.
- Pupils have their own individual school issued accounts using Google Apps for Education. The forwarding of chain emails is not permitted in school.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission and virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.
- Staff must inform (the Vice Principal or line manager) if they receive an offensive e-mail. Pupils are introduced to e-mail as part of the Computing Programme of Study.

- However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the School e-mail policies apply.

APPENDIX 4

Acceptable Use Agreement / e-Safety Rules

Pupils – Junior School (Reception to Year 4)

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address.
- I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the School community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the day
- I will not sign up to online services until I am old enough.

Acceptable Use Agreement:

Pupils - Junior School (Years 5 & 6)

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the School network, other systems and resources with my own username and password
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I am aware that when I take images of pupils and/or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the School network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the School
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the School's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers and/or parents
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

17 49

ST MARGARET'S

SCHOOL

Dear Parent (Junior School, Rec – Year 6),

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Mrs E Gray (Head of Junior School).

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Parent signature (Junior School, Rec – Year 6)

We have discussed this document with *(child's name)*

and we agree to follow the acceptable use/ e-Safety rules and to support the safe use of ICT at St Margaret's School.

Parent Signature: …….

Form: Date:

Completed copies of this form should be returned to the IT Manager via the Class Teacher at St Margaret's School.

Appendix 5

Acceptable Use Agreement:

Pupils – Senior School

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the School network, other systems and resources with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by a teacher.
- I am aware that when I take images of pupils and/or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the School network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the School.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the School community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the School community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers and/or parents.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

17 49

ST MARGARET'S

SCHOOL

Dear Parent (Senior School Years 7 – 13),

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Miss J Chatkiewicz (Vice Principal).

Please return the bottom section of this form which will be kept on record at the School.

Parent signature (Senior School Years 7 – 13)

We have discussed this document with *(child's name)*

and we agree to follow the acceptable use/ e-Safety rules and to support the safe use of ICT at St Margaret's School.

Parent Signature: ……

Pupil Signature: ……

Form: ……. Date:

Completed copies of this form should be returned to the IT Manager via the Form Tutors at St Margaret's School.