St Mary's School
CAMBRIDGE

On-line Safety Policy

This policy is the responsibility of the *Designated Safeguarding Lead and the IT Director.*

On-line safety procedures and the education of pupils about keeping safe on-line are included in the Governors' annual review of safeguarding.

Last review: September 2020.

Next review: September 2021

Introduction

It is the duty of St Mary's School, Cambridge ('the School') to ensure that every pupil in its care (from EYFS up to and including Sixth Form and boarders) is safe; and the same principles apply to the digital world as apply to the real world.

IT and on-line 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 on-line environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, discrimination, 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 but is not limited to: websites, email and instant messaging, blogs, on-line learning platforms, social networking sites, cloud technologies, chat rooms, music/video downloads, gaming sites, text messaging and picture messaging, video calls, podcasts, on-line communities, and mobile internet devices such as smart phones and tablets.

The following School policies, procedures, and materials can be found on the School website policies are relevant to this policy:

- *Safeguarding and Child Protection Policy*
- *Staff Behaviour Policy*
- *IT Acceptable Use Policy*
- *Pupil Internet and IT Acceptable Use Policy*

- *Health and Safety Practical arrangements Policy*
- *Behaviour, Discipline and Exclusions Policy*
- *Anti-Bullying Policy*
- *Whistleblowing Policy*
- *Social Media Policy*
- *Staff Data Protection Policy*
- *Bring Your Own Device Policy*
- *PSHEE Policy*
- *Arrangements for Risk Assessments Policy*
- *Information on Data Security, data sharing, retention, and deletion*

This policy has regard to the following advice and guidance:

Keeping Children Safe in Education (DfE September 2020)

Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE 2019)

Guidance for Safer Working Practice for Adults who work with Children and Young people in Education 2019 (Safer Recruitment Consortium May 2019)

Information Sharing advice for practitioners providing safeguarding services (DofE July 2018)

Sexual Violence and Sexual Harassment between children in schools and colleges (DfE May 2018)

Preventing and Tackling Bullying (DfE July 2017)

Sexting in Schools and Colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016)

Prevent duty guidance for England and Wales (Home Office, July 2015)

Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, April 2015).

The School understands the responsibility to educate our pupils on on-line 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 on-line safety and listening to their fears and anxieties as well as their thoughts and ideas.

On-line safety depends on effective practice at several levels:

- Responsible IT use by all Staff, volunteers, visitors, and pupils
- Sound implementation of on-line safety policy in both administration and across the curriculum
- Safe and secure internet access including the effective management of filtering and monitoring of software.
- Education of everyone in our School community regarding safe practice
- Security of sensitive data and information

- Adherence to the IT Acceptable Use Policy and the Pupil Internet and Information Technology Acceptable Use Policy.

Scope of this Policy

This policy applies to all members of the School community, including Staff, all pupils (including boarders), parents and visitors, who have access to and are users of the School technology systems or otherwise use technology for viewing or exchanging information in a way which affects the welfare of pupils or any member of the School community or where the culture or the reputation of the School is put at risk. In this policy 'Staff' includes teaching and non-teaching Staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

Both this policy and the IT Acceptable Use Policy (for all Staff, volunteers, and visitors) and the Pupil Internet and Information Technology Acceptable Use Policy cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, chrome books, 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, chrome books, tablets, smart phones, etc.).

The School's policies apply to the use of technology by all Staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture of reputation of the School is put at risk.

Roles and responsibilities

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 undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies.

The link governor for safeguarding is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's approach to on-line safety and the use of technology within the School, on behalf of the Governing Body.

Head and the Senior Leadership Team (SLT)

The Head is responsible for the safety of the members of the School community, and this includes responsibility for on-line safety. The Head has delegated day-to-day responsibility to the Designated Safeguarding Lead at the Senior School, who is a member of the SLT.

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

- Staff, in particular the DSL at the Junior and Senior School and the IT Director are adequately trained about on-line safety
- Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of on-line safety in connection to the School.

Designated Safeguarding Lead

The School's Designated Safeguarding Lead (senior School) is responsible to the Head for the day-to-day issues relating to on-line safety. The Designated Safeguarding Lead (senior school) includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters. The Designated Safeguarding Lead (senior school) works with the DSL in the junior school, the IT Director, and

the Head of the senior school to monitor technology uses and practices to assess if improvements can be made to ensure the on-line safety and wellbeing of pupils. The Designated safeguarding lead (senior school) will regularly monitor the technology incident log maintained by the IT Director and will regularly update other members of the School's Senior Management Team and the Governing Body on the School's safeguarding arrangements, including on-line safety practices. The Designated Safeguarding Lead (senior school) has a responsibility to carry out a risk assessment where a concern about a pupil's welfare is identified and to ensure that the relevant findings are implemented, monitored, and evaluated.

IT Staff

The School's technical Staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. The IT Director, together with the IT team 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 Designated Safeguarding Leads or Head as appropriate. The IT Director is responsible for ensuring that:

- The School's technology infrastructure is secure and so far, as possible, is not open to misuse or malicious attack.
- The user may only use the School's technology if they are properly authenticated and authorised.
- The School has an effective monitoring and filtering policy in place and that is applied and updated on a regular basis.
- The risks of pupils and Staff circumventing the safeguards put in place by the School are minimised.
- The use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
- Monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the School's network and maintain logs of such use.

The IT Director will report to the SLT on the operation of the School's IT and if he has concerns about the functionality, effectiveness, suitability or use of IT within the School he will escalate those concerns to the appropriate member of SLT. The IT Director is responsible for maintaining the Technology Incident log and bringing any matters of safeguarding concern to the attention of the DSL / Head as appropriate and in accordance with the School's *Safeguarding and Child Protection Policy*.

All Staff

Staff are expected to adhere to each of the policies referred to in this policy.

Staff are responsible for promoting and supporting safe behaviours in their classrooms, and that supervision is appropriate. As with all issues of safety at this School, Staff are encouraged to create a talking and listening culture in order to address any on-line safety issues which may arise in classrooms on a daily basis.

Staff have a responsibility to report any concerns about on-line safety or a Pupil's welfare and safety in accordance with this policy and the School's *Safeguarding and Child Protection Policy*.

Pupils

Pupils are responsible for using the School IT systems in accordance with the Pupil Internet and Information Technology Acceptable Use Policy, and for letting Staff know if they see IT systems being misused.

Parents and carers

It is essential for Parents to be fully involved with promoting on-line safety both in and outside of School. We engage with Parents and seek to promote a wide understanding of the benefits and risks related to internet usage. Parents are encouraged to support the School in the implementation of this policy and the *Pupil Internet and Information Technology Policy* and report any concerns in line with the School's policies and procedures. Parents are encouraged to talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour and should encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support. 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 or ask if any information about on-line safety is required.

Education and training

Staff: awareness and training

New Staff receive information on the *IT Acceptable Use Policy*, the *On-line Safety Policy* and *Staff Behaviour Policy* as part of their induction.

All teaching Staff receive regular information and training on on-line 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 children within the context of on-line safety. All supply Staff and contractors with access to and who are users of the School IT systems receive information about on-line safety as part of their safeguarding briefing on arrival at School.

Staff also receive data protection guidance on induction and at regular intervals afterwards.

All Staff working with children are responsible for demonstrating, promoting, and supporting safe behaviours in their classrooms and following school on-line safety procedures. These behaviours are summarised in the *IT Acceptable Use Policy* which must be signed and returned before use of technologies in School. When children use School computers, Staff should make sure the *Pupil Internet and Information Technology Policy* is understood and adhered to.

Teaching Staff are encouraged to incorporate on-line 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 logging of concern form must be completed by Staff as soon as possible if any incident relating to on-line safety occurs. This will be completed on using **MyConcern** and will be provided directly to the School's Designated Safeguarding Lead or Head in accordance with the *Safeguarding and Child Protection Policy*.

Pupils: on-line safety in the curriculum

The safe use of technology is integral to the School's curriculum. The School provides opportunities to teach about on-line safety within a range of curriculum areas and IT lessons.

Educating pupils on the dangers of technologies that may be encountered outside School will also be carried out via the pastoral and PSHEE programme, by presentations in assemblies, as well as informally when opportunities arise.

In the Junior School children are guided to recognise technology is in places such as homes and schools and they are encouraged to select and use technology for particular purposes.

At the senior school, at age-appropriate levels, and usually via PSHEE, pupils are taught about the importance of safe and responsible use of technology, about their on-line safety responsibilities and to look after their own on-line safety, how to recognise cyberbullying and prejudice based bullying, the impact of this and how and who to report it, about recognising on-line sexual exploitation, stalking and grooming, the risks, and the importance of reporting and any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Lead, the IT Director, and any member of Staff at the School.

Pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property and the consequences of negative on-line behaviour. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

The *Pupil Internet and Information Technology Acceptable Use Policy* details the School rules about the use of technology, including internet, email, social media, and mobile devices, helping pupils to protect themselves and others when using IT. Pupils and parents are reminded of the content of this policy on a regular basis and at the start of each academic year.

Parents

Parents are encouraged to read the *Pupil Internet and Information Technology Acceptable Use Policy* with their child to ensure that it is fully understood. Parents of Junior School pupils are required to read and sign this policy. Pupils at the senior school are required to read and sign this policy.

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 annual discussion evenings for parents when a member of SLT or an outside specialist advises about on-line safety and the practical steps that parents can take to minimise the potential dangers to their child without curbing their natural enthusiasm and curiosity. Useful resources about the safe use of technology are available via various websites including:

- http://www.thinkuknow.co.uk
- http://www.disrespectnobody.co.uk
- http://www.saferinternet.org.uk/advice-centre/parents-and-careres
- http://www.internetmatters.org
- http://educateagainsthate.com
- http://www.kidsmart.org.uk
- http://www.safetynetkids.org.uk
- http://www.safekids.com
- http://parentinfo.org
- Department of Education advice on Cyberbullying

Policy Statements

Access to the School's technology and use of school and personal devices.

The School provides internet, intranet access and email systems to pupils and Staff as well as other technology. Pupils must comply with the *Pupil Internet and IT Acceptable Use Policy* and Staff must comply with the *IT Acceptable Use Policy* when using School technology. All such use is monitored by the IT department.

Staff

School devices assigned to a member of Staff as part of their role must have an individual password, username, and device lock so that unauthorised people cannot access the content. When Staff 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 Staff and Visitors *Bring your own device Policy* for further guidance on the use of non-School owned electronic devices for work purposes.

Staff at St Mary's School, Cambridge, are permitted to bring in personal devices for their own use. Devices should not be used in the classroom/teaching areas. The use of any personal device connected to the School's Wi-Fi network will be logged and monitored by the IT department.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may Staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

The *Pupil Internet and Information Technology Acceptable Use Policy* and rules for each year group govern the use of School - issued and personal mobile devices. 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 pupils' 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.

Use of internet and email

Staff, Parents and Visitors (as applicable)

Staff must not access social networking sites, or any website or personal email which is unconnected with schoolwork or business from School devices or whilst teaching or in front of pupils. Such access may only be made from Staff members' own devices whilst in Staff-only areas of School.

When accessed from Staff members' own devices / off School premises, Staff must use social networking sites with extreme caution, being aware of the nature of what is published on-line and its potential impact on their professional position and the reputation of the School.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that email communications through the School network and Staff email addresses are monitored.

Only the School's email system should be used for any school-related business, including communications with pupils, Parents and Visitors.

Staff, Parents and Visitors must immediately report to Designated Safeguarding Lead, member of SLT or the IT Director, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Staff, Parents and Visitors must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Director or member of the IT team. Attachments to emails should not be

opened unless the source is known and trusted. The forwarding of chain emails, including jokes, advertisements or promotional offers is not allowed.

Staff, Parents and Visitors must not access, create, display, download, distribute, store, edit or record any material, including images, that is illegal, deceptive, or likely to offend other members of the School community, for example, content that can constitute any forms of unlawful discrimination, obscene, pornographic, or paedophiliac, or promotes violence, discrimination, or extremism.

Any on-line communications must not either knowingly or recklessly:

- place a child or young person at risk of harm or cause actual harm.
- bring St Mary's, Cambridge into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual.
- make offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, pregnancy or marital status, religion or belief or age
- use social media to bully another individual.
- post links to or endorsing material which is discriminatory or offensive.

For members of Staff, under no circumstances should School pupils or Parents be added as social network 'friends' or contacted through social media. For Parents and Visitors no School pupil should be added as social network 'friends' or contacted through social media.

Any digital communication between Staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may Staff contact a pupil or parent / carer using any personal email address. The School ensures that Staff have access to their work email address when offsite, for use as necessary on School business.

Staff, Parents and Visitors must not install or attempt to download and install software of any type on the School IT devices/system without seeking the prior permission of the School's IT Director.

Staff, Parents and Visitors are not permitted to download or install screensavers on the School's computers or portable devices.

Staff, Parents and Visitors are not permitted to use the School's IT facilities to download or store videos or images for personal use.

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 school email service may be regarded as safe and secure, and must be used for all School work, assignments, research projects. Pupils are made 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 School work / research purposes, pupils should contact the IT team 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 Designated Safeguarding Lead/ IT Director / or another member of Staff.

The School expects pupils to think carefully before they post any information on-line or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate, discriminatory, 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 Designated Safeguarding Lead / IT Director / 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 policies and procedures (in particular the *Behaviour Management Policy*, *Discipline, Exclusions and Required Removal Policy*, *Safeguarding and Child Protection Policy* and *Anti-bullying Policy*). Pupils should be aware that all internet usage via the School's systems and its wi-fi network is monitored.

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

Data protection – storage, processing and record keeping

Staff are referred to the *Staff Data Protection Policy* and the Guidance on data breach and retention and deletion guidelines on the St Mary's cloud in the All Staff - Data Protection tile. Staff and pupils are expected to save all data relating to their work to their School laptop/ PC / School - issued device.

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 school IT equipment offsite when authorised to do so by the IT Director, and only when it is necessary and required in order to fulfil their role.

Staff, Parents and Visitors are reminded of the importance of maintaining the security of the School's IT network and the data. The following steps must be taken:

- When leaving a room Staff, Parents and Visitors should log off from any School computer or other School device or device they have been using to access School data.
- Any portable device must be taken from the room.
- Staff, Parents and Visitors must only access the School IT system using their own user name and password and such information must not be shared.

When using email, the following should be noted:

- Some email software will suggest names of people who have been emailed before; make sure you chose the right address/name before sending.
- Know how to use blind copy (bcc) correctly and if in doubt ask advice from the IT team. This should be used with care as recipients may not appreciate that they have been blind copied and may reply to all. In general, it is better to use forward email function with an explanation.
- Exercise care with 'reply all' and group email addresses to ensure you do want to send your email to all in the group. Note that 'reply all' in 365 will send to all those who were part of this email chain even if some people have not been copied in recently sent parts of the chain. If in doubt, start a fresh email.
- Check email addresses and whether the email is secure before sending an email.

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)
- not write passwords down
- not share passwords with other pupils or Staff.

Safe use of digital and video images and copyright

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 can take digital / video images to support educational aims, but must follow this policy, the *IT Acceptable Use Policy and Taking*, *Storing and Using Images of Children 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 without express permission.

Written permission from parents or carers will be obtained before photographs of Pupils are published on the School website (see Parent Contract for more information).

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.

Copyright applies to all text, pictures, video, and sound, including those sent by email or on the internet. Files containing copyright-protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material.

Misuse by Pupils, Staff or any user

Staff, pupils, and parents are required to report incidents of misuse or suspected misuse to the School is accordance with this policy and the Schools Safeguarding and Child Protection Policy and Whistleblowing Policy. The School reserves the right to withdraw access to the School's IT network/systems by any user at any time. The 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 SCPB. If the School discovers that a child or young person is at risk because of on-line activity, it may seek assistance from the CEOP.

Misuse by Pupils

Anyone who has any concern about the misuse of technology by Pupils should report it so it can be dealt with in accordance with the School's policies and procedures (in particular the *Safeguarding and Child Protection Policy*, *On-Line safety Policy*, *Anti-bullying Policy* (where there is an issue of cyberbullying) and the *Behaviour Management Policy* and *Discipline, Exclusions and Required Removal Policy*.

Misuse by Staff

Anyone who has any concern about the misuse of technology by Staff should report it in accordance with the School's *Whistleblowing Policy* so it can be dealt with in accordance with the Staff disciplinary procedures. If anyone has a safeguarding-related concern relating to Staff misuse of technology, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against Staff set out in the School's *Safeguarding and Child Protection Policy*.

Misuse by any user

Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Director of IT, the Designated Safeguarding Lead or the Head. The School reserves the right to withdraw access to the School's network at any time and to report suspected illegal activity to the police. If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. Any person who has a concern relating to extremism may report it directly to the police.