St Mary's School
CAMBRIDGE

Online Safety Policy

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

Online safety procedures and the education of pupils about keeping safe online are included in the Governors' annual review of safeguarding.

Last review: March 25

Next review: September 25

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 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 (including cyber, prejudice – based and discriminatory bullying), harassment, discrimination, grooming, stalking, abuse, and radicalisation.

Modern 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 are not limited to websites, email and instant messaging, blogs, online learning platforms, social networking sites, cloud technologies, chat rooms, music/video downloads, gaming sites, text messaging and picture messaging, video calls, podcasts, online communities, and mobile internet devices such as smart phones and tablets.

The following School policies, procedures and materials are relevant to this policy and can be found either on the school website or on St Mary's Cloud:

- *Safeguarding and Child Protection Policy*
- *Staff Behaviour Policy*

- *IT Acceptable Use Policy*
- *Pupil Internet and IT Acceptable Use Policy*
- *Acceptable Use of Artificial Intelligence Policy*
- *Health and Safety Practical Arrangements Policy*
- *Behaviour Management Policy*
- *Discipline, Exclusions and Required Removal 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*

This policy has regard to the following advice and guidance:

Keeping Children Safe in Education (DfE September 2024)

Teaching online safety in schools (DfE June 2019 – updated Jan 2023)

Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE 2021)

Guidance for Safer Working Practice for Adults who work with Children and Young people in Education

Information Sharing advice for practitioners providing safeguarding services (DofE May 2024)

Preventing and Tackling Bullying (DfE July 2017)

Searching, screening and confiscation: advice for schools (DfE Updated: July 2023)

Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfE: updated March 2024)

Harmful online challenges and online hoaxes (DfE February 2021)

Online Safety guidance if you own or manage your own online platform (DfDCMS, June 2021)

A business guide for protecting children on your online platform (DfDCMS, June 2021)

Online safety audit tool (UKCIS Updated: October 2022)

Online safety act (2023)

Prevent duty guidance for England and Wales (Home Office, March 2024)

Channel duty guidance: protecting people from being drawn into terrorism (Home Office, updated December 2023).

The School understands its responsibility to educate our pupils on online 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 online safety and listening to their concerns as well as their thoughts and ideas.

Online safety depends on effective practice at several levels:

- Responsible IT use by all Staff, volunteers, visitors, and pupils
- Sound implementation of online 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 including information for parents/carers
- 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 the Early Years Foundation Stage (EYFS) and boarders), parents/carers and visitors, who have access to and are users of school technology systems or otherwise use technology for viewing or exchanging information in a way which affects the welfare or wellbeing 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 or wellbeing of other pupils or any member of the school community or where the culture or 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 its 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 online 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 online 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, the Digital Strategy Lead and the IT Director are adequately trained about online safety
- Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online 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 online 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 Digital Strategy Lead, the IT Director, the Head, and the Head of Juniors to monitor technology uses and practices to assess if improvements can be made to ensure the online 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 Leadership Team and the Governing Body on the School's safeguarding arrangements, including online safety practices. The Designated Safeguarding Lead will work with others to decide what information is given to parents about online safety and the monitoring and filtering that takes place in school. The Designated Safeguarding Lead (Senior School) has a responsibility to carry out a risk assessment where a concern about a pupil's welfare or wellbeing 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, is 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 staff understand how to effectively monitor use in the classroom.
- 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 they have concerns about the functionality, effectiveness, suitability, or use of IT within the School they 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 online behaviours and have a responsibility to act as good role models in their use of technology and understand that supervision is appropriate. As with all issues of safety at this School, staff are encouraged to create a talking and listening culture to address any online safety issues which may arise on a daily basis.

All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face to face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

Staff are expected to be alert to the possibility of pupils abusing other children online and to understand that this can occur both inside and outside of school. Examples can include:

- sending of abusive and or harassing messages
- the consensual and non-consensual sharing of nudes and semi-nude images and videos which is sometimes known as sexting or youth produced sexual imagery
- the sharing of abusive images and pornography; and
- Cyber bullying (which may include prejudice- based or discriminatory bullying)

Staff are also aware that many other forms of abuse may include an online element such as that which:

- Facilitate, threaten and or encourage physical abuse, sexual violence or is used as part of initiation hazing type violence and rituals.

Staff understand that it is important for them to recognise the indicators and signs of peer-on-peer abuse and that they know how to identify it and respond to reports. Staff challenge inappropriate behaviours between children and do not downplay certain behaviours as banter or part of growing up as they recognise that doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and lead to a culture that normalises abuse. The school has a zero-tolerance approach towards peer-on-peer abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated.

Staff have a responsibility to report any concerns about online safety or a pupil's welfare, wellbeing, and safety in accordance with this policy and the School's *Safeguarding and Child Protection Policy*. If staff have any concerns about peer-on-peer abuse or are unsure of what to do in a particular incident they should speak to a Designated Safeguarding Lead.

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 online 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 wellbeing 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 online safety is required.

Online Safety

The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the Designated Safeguarding Lead. The term 'online safety' encapsulates a wide range of issues but these can be classified into four primary areas of risk:

(a) Content - being exposed to illegal, inappropriate, or harmful content (e.g. pornography, fake news, deepfakes, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism);

(b) Contact - being subjected to harmful online interaction with other users (e.g. peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);

(c) Conduct - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending, and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

(d) Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Education and training

Staff: awareness and training

New staff receive information on the *IT Acceptable Use Policy*, the *Online Safety Policy,* and *Staff Behaviour Policy* as part of their induction. New staff complete an e-learning course on online safety.

All teaching staff receive regular information and training on online safety issues in the form of induction, INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi nudes, images and all videos, cyber bullying and radicalisation and dealing with harmful online challenges and hoaxes. All supply staff and contractors with access to and who are users of the School IT systems receive information about online safety as part of their induction 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 online behaviours and following school online 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 online 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 online safety for a student occurs. This will be completed 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. In the case of a concern regarding another member of staff a low-level concern should be completed, where a member of staff feels they may be in a difficult or potentially compromising situation they should always complete the self-reporting form.

Where pupils wish to report a safeguarding concern, all staff are taught to reassure those involved that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in with safeguarding and wellbeing issues, including those involving the use of technology and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

Where safeguarding incidents involving online elements, such as youth produced sexual imagery, staff will not view, or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos are set in the School's *Safeguarding and Child Protection Policy* and the *Search and Confiscation Policy.*

Staff are encouraged to adopt and maintain an attitude of 'it could happen here' in relation to sexual violence and sexual harassment and to address inappropriate behaviours. Staff are trained to look out for potential patterns of concerning inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and staff training will be delivered to minimise the risk of it happening again.

Useful online resources for staff (in addition to the links above):

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

https://www.childnet.com/teachers-and-professionals

Keeping children safe online | NSPCC

https://thinkuknow.co.uk/teachers/

https://educateagainsthate.com/

Common Sense Education

Home | Tooled Up Education

Professionals' online safety helpline: helpline@saferinternet.org.uk Tel: 0344 381 4772

Internet Watch Foundation – internet line for the public and IT professionals to report potentially criminal online content

SCPB guidance on radicalisation

Pupils: online safety in the curriculum

The safe and responsible use of technology is integral to the School's curriculum. The School provides opportunities to teach about online safety in an age-appropriate manner within a range of curriculum areas.

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 (and in the educational programmes followed in the EYFS), children are guided to recognise technology is in places such as homes and schools and they are encouraged to select and use technology for purposes. They are guided to make sense of their physical world through opportunities to explore, observe and find out about people, places technology and the environment. Pupils explore and play with a wide range of media and are provided with opportunities for sharing their thoughts through a variety of activities which include safe use of technology.

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 online safety responsibilities and to look after their own online safety and that of other children, how to recognise cyberbullying, prejudice-based and discriminatory bullying or extremist behaviour, the impact of this and how and to whom to report it, about recognising online sexual exploitation, stalking and grooming, the risks, and the importance of reporting any such instances they or their peers come across whether on or offline. Pupils are taught how to report any incidents that make them feel uncomfortable or under threat and how the School will deal with those who behave badly. They are also taught about how to deal with harmful online challenges and hoaxes. Pupils can report concerns to the Designated Safeguarding Lead, the IT Director, the Director of Digital Learning, and any member of staff at 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 online behaviour. Pupils are taught about respecting other people's online information and images (etc.) through discussion and classroom activities.

Pupils are taught about the risks associated with all forms of abuse including physical abuse and sexual violence and sexual harassment which may include an online element. The school has a zero-tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's *Behaviour Management Policy* and also as a safeguarding matter under the School's *Safeguarding and Child Protection Policy* and procedures.

The safe use of technology aspects of the curriculum is reviewed on a regular basis to ensure its relevance.

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.

Useful online safety resources for pupils:

- https://www.thinkuknow.co.uk
- https://www.childnet.com/young-people
- https://www.saferinternet.org.uk/advice-centre/young-people
- https://mysafetynet.org.uk/

- https://www.bbc.com/ownit
- https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/
- https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people

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 online 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:

- https://www.thinkuknow.co.uk/parents/
- https://www.saferinternet.org.uk/advice-centre/parents-and-carers
- https://childnet.com/parents-and-carers
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- https://www.internetmatters.org/
- https://educateagainsthate.com
- Safety Net
- https://www.safekids.com
- https://parentzone.org.uk/
- Online safety and advice resources
- https://www.commonsensemedia.org/
- Ask About Games
- https://www.ceop.police.uk/safety-centre
- Department of Education advice on Cyberbullying
- Home | Tooled Up Education

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. it is broadly categorised as either ‘cyber-enabled’ (crimes that can happen offline but are enabled at scale and online) or cyber - dependent (crimes that can be committed only by using a computer).
Cyber- dependent crimes include

- unauthorised access to computers (illegal ‘hacking’), for example, accessing a school’s computer network to look for test paper answers or change grades awarded;
- denial of service (Dos or DDoS) attacks or ‘booting’ which are attempts to make a computer, network, or website unavailable by overwhelming it with internet traffic from multiple sources; and

- making, supplying, or obtaining malware (malicious software) such as viruses, spyware, ransomware botnets ad Remote Access Trojans with the intent to commit further offences, including those above.

Pupils may inadvertently or deliberately stray into cyber- dependent crime and if staff have any concerns they should refer to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead should then consider referring onto the cyber choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber - dependent offences and divert them to a more positive use of their skills and interests. Cyber choices do not currently cover cyber - enabled crime such as fraud, purchasing of illegal drugs online and child sexual abuse and exploitation nor other areas of concern such as online bullying or general online safety.

Risk Assessment

Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified. Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused. The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated. Day to day responsibility to carry out risk assessments under this policy will be delegated to Deputy Head (Pastoral and Boarding), Head of Boarding, or Head of Juniors (as appropriate) who have been professionally trained in and tasked with carrying out the particular assessment.

Record Keeping

All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records. All serious incidents involving the use of technology will be logged centrally on **MyConcern** and in the IT incident log by the Director of IT as part of the pupil or staff record.

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 which are only to be used for the purpose of multi-factor authentication 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. Please see the Staff Behaviour Policy for more information.

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 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.

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 online 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 School 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 online 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 School, 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, 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 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 schoolwork, 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 schoolwork / 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 / Digital Strategy Lead 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, 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 (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 schoolwork / 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 username 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 choose 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 and/or symbols)
- not write passwords down
- change passwords regularly
- 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. 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 and stored 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 in accordance with this policy and the School’s *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 online 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*, *Online 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 Director of Digital Learning, 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.