



# **St Mark's West Essex Catholic School**

## **E-Safety Policy**

**Date Reviewed: July 2017**

**Next Review Date: July 2019**

**Committee: Curriculum, Pupils and Admissions**

St Mark's believes that online safety (E-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. Internet and information communication technologies are an important part of everyday life, so children must learn how to develop strategies to manage and respond to risk and be empowered to build resilience online. We have a shared responsibility to ensure that all pupils and staff are protected from potential harm online.

The purpose of the E-Safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the responsible use of technology to ensure that St Mark's is a safe and secure environment.
- Help safeguard and protect all members of the St Mark's community online by ensuring training and education and monitoring, as well as, filtering pupil activity on the internet.
- Raise awareness with all members of the school community regarding the potential risks as well as the benefits of technology.
- Enable all staff to work safely and responsibly, to model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

### **Teaching and Learning**

The internet is essential for education, business and social interaction. St Mark's has a duty to provide pupils with internet access as part of their learning experience. Internet access at St Mark's is designed expressly for pupil use and is a part of the statutory curriculum. It is a necessary tool for staff and pupils.

Pupils will be educated in the effective and appropriate use of the internet:

- They will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- They will be taught to be selective when accessing the internet, helping to ensure that the content they search for and view is appropriate and legal and in line with the E-Safety policy.
- There will be lessons on internet-related issues, and pupils should be taught to know the risks, affects and morals involved in such a way as to help and encourage them to make safe and appropriate choices on the internet. They will be taught about the dangers of social media.

-- Pupils will also be taught to be selective when accessing sites suggested by search engines and advertisements – i.e. to make a preliminary check of likely content for appropriateness and not to simply blindly click to enter a site.

-- Pupils will be instructed that if they accidentally access inappropriate material they should tell a responsible adult immediately.

### **Managing Internet Access**

The network manager will ensure the supply of a safe and secure broadband connection. The ICT system's capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly. The filter will be kept up-to-date. Any misuse will be reviewed and necessary steps will be taken with those breaking rules.

### **Managing filtering**

St Mark's will monitor all content accessed via the internet in school. If staff or pupils discover an unsuitable site, it must be reported to the network manager. ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. All monitoring of school owned/provided systems will take place to safeguard members of the community. The school uses educational filtered secure broadband connectivity, which is appropriate to the age and requirements of our pupils.

### **Managing emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones will be handed into the office at the start of each school day (Years 7-11). Years 12-13 should switch off their mobile phones during lessons or other formal school time. The sending of inappropriate or abusive text messages or email is forbidden, as is the videoing or photographing without permission of others on school property/business.

Users bringing mobile devices into school must ensure there is no inappropriate or illegal content on the device. The school is not responsible for the theft, damage or loss of any mobile device.

### **E-mail / Messaging**

All pupils and staff have an individual school email address, and with it, access to the Microsoft 365 suite of applications. Pupils and staff also have individual logins for the Showmyhomework online platform which is used for setting homework and which has a messaging facility.

The following must be observed:

-- The school-provided email accounts and the messaging function in Showmyhomework are to be used for educational purposes and school business only.

-- Staff must use the school email address for any official communication. The use of personal email addresses by staff for any school business is not permitted. All email is filtered and logged; if necessary e-mail histories can be traced.

-- It is the responsibility of each account holder to keep all passwords secure. Pupils will be advised on security and encouraged to change passwords regularly.

-- **Any electronic communication is a formal communication between the school and the recipient. It must therefore adhere to the highest professional standards.** All communications via email or the Showmyhomework messaging system should be written carefully, in the same way as a letter written on school headed paper would be. Pupils and staff are expected to use appropriate language and not to reveal any personal details about themselves or others in electronic communication.

-- Pupils must immediately tell a teacher if they receive an offensive e-mail; staff must inform a member of the senior leadership team. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

-- Access to school email systems and the messaging function in Showmyhomework will always take place in accordance with data protection legislation and in line with other school policies.

-- Staff are encouraged to develop an appropriate work-life balance when communicating with pupils or parents via email or messages. Staff are not expected to respond to emails or messages outside of working hours and should not feel pressured to do so.

-- Emails used for internal communication should be kept to a minimum and only used for non-sensitive issues.

-- School email addresses and other official contact details may not be used for setting up personal social media accounts. The use of Hotmail, BT Internet, Yahoo, Google or any other Internet based webmail service for sending e-mails concerning school business is not permitted.

-- Staff and pupils must never open attachments from an untrusted source.

-- E-mails created or received in school are subject to disclosure in response to requests under the Freedom of Information Act 2000. This reinforces the need for professionalism at all times.

### **Online learning platforms**

Senior leaders will monitor usage of online learning platforms, such as Showmyhomework. Pupils and staff will be advised about acceptable conduct and use. All users will be mindful of copyright issues and will only upload appropriate content.

Any concerns about content or messages on the platform will be recorded and dealt with in the following ways:

- a) The user will be asked to remove any content or message deemed to be inappropriate.
- b) The material will be removed by the site administrator if the user does not comply.
- c) Access to the platform for the user may be suspended.
- d) The user will need to discuss the issues with a senior leader before reinstatement.
- e) A pupil's parent/carer may be informed.

### **Published content and the school web site**

The contact details on the web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupils' images and work**

The school will ensure that all images and videos shared online are used in accordance with the school image use policy. Written consent from parents or carers is sought when a pupil joins the school for publishing images or videos of pupils on the website or in other school publications. Pupils' work can only be published with the permission of the pupil.

### **Social media**

St Mark's does not use social networks as part of the curriculum or for information purposes. However, pupils are taught in PSHE and ICT lessons about the potential dangers of social media (blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others).

-- Social media should never be used in a way that breaches any of the school's other policies, for example: this policy; the Code of Conduct; the Behaviour Policy or procedures; the Anti-bullying Policy; the Equality Scheme; the Data Protection Policy; any other laws or regulatory requirements.

- Pupils and staff are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or which may bring the school into disrepute.
- Pupils and staff are advised never to give out personal details of any kind; to deny access to unknown individuals; to block unwanted communications; to invite known friends only and deny access to others when using social media.
- All members of staff are advised not to communicate with or add as 'friends' any current/past pupils or current/past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the designated safeguarding lead and/or the headteacher.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted. Any communication from pupils or parents received on personal social media accounts will be reported to the school's designated safeguarding lead.
- Use of social media whilst using school devices may result in disciplinary or legal action and removal of internet facilities.
- Any concerns regarding the online conduct of any member of the St Mark's community on social media sites should be reported to the senior leadership team.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with the relevant policies.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location-sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with the school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework. It is important to ensure that any social media posts are in a personal capacity, rather than referring in any way to the school, senior leadership team or governing body.

-- Members of staff will notify the senior leadership team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

### **Authorising internet access**

St Mark's will maintain a current record of all staff and pupils who are granted access to school ICT systems. Access to the ICT resources and/or the internet will be withdrawn should the system be used inappropriately.

### **Assessing risks**

St Mark's will take all reasonable precautions to prevent access to inappropriate material using school equipment/resources. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

### **CCTV**

The school uses CCTV for security and safety. The only people with access to this are identified members of the senior leadership team and the site team manager. Notification of CCTV use is displayed around the school.

### **Handling E-Safety complaints**

Complaints of internet misuse will be dealt with by the network manager or the senior member of staff responsible for ICT. Any complaint about staff misuse must be referred to the deputy headteacher with responsibility for the school's ICT network and systems. Complaints of a child protection/safeguarding nature must be dealt with in accordance with school's safeguarding procedures.

### **Protecting personal data**

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

### **Introducing the E-Safety policy to pupils**

Pupils will be informed that network and internet use within the school system will be monitored. Pupils will be informed about the content of this policy.

### **Staff and the E-Safety policy**

Staff will be informed about the content of this policy and will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential. Staff who monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Where it is suspected that a pupil is at risk from internet abuse or cyberbullying, staff will report concerns in line with safeguarding procedures.

### **Parental partnership**

Parents and carers have a crucial role to play in their child's safety online and in their use of the internet and mobile communication.

The school strongly advises that parents and carers ensure that they have the appropriate skills, knowledge and resources to monitor their child's online activity and that they keep up-to-date with these rapidly changing communication technologies. The complementary support to that obtained in school will help to guide young people through this potentially difficult area. St Mark's encourages any parent or carer who has concerns to contact the school to discuss and resolve issues where necessary.

The school will endeavour to support the process of mutual support in the sharing of updates and information through channels such as the newsletter, school website and parent evenings.