St Mary's Academy Trust

Policy for e-safety

May 2018

Background and Introduction:

This policy was drafted following guidance from the LA and BECTA.

The policy was updated in light of Ofsted document 'The Safe Use of New Technologies' February 2010 and with the support and advice from CEOP (The Child Exploitation and Online Protection Centre).

The policy will aim to:

- Clarify the schools approach to e-safety for all staff and pupils.
- Reinforce the e-safety of pupils and others regarding the use of electronic media (internet, mobile phones and devices with wireless access).
- Encourage pupils to take responsibility for themselves when using new technologies.
- Give guidance on developing, implementing and monitoring the e-safety education programme which builds on what they have learnt before and reflects their age and stage of development.
- Enable staff to manage e-safety issues on school premises, and any incidents that occur with confidence, consistency, and in the best interests of those involved
- Ensure that the response to incidents involving e-safety complements the overall approach to E-safety education and the values and ethos of the school.

This policy applies to all staff, pupils, parents, governors and partner agencies working with the school.

Staff with Key Responsibility for E-safety:

- It is the responsibility of all staff members for the management for e-safety incidents and the provision of e-safety education.
- The e-Learning Leader will take a lead in updating and disseminating the policy to staff and governors.
- The most senior member of staff available will deal with any e-safety related incident as described in this policy.
- Individual teaching staff ensure that appropriate e-safety education is provided in line with arrangements specified below.

E-safety Education:

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access:

Information system security

School currently uses a lockdown system meaning that websites deemed unsuitable are inaccessible. However, we recognise that this is less effective at helping them to learn how to use new technologies safely than a managed system (which does not restrict access). This might ultimately mean that pupils are more vulnerable overall when using the internet unaided as they do not know how to manage unexpected content, (Ofsted Guidance February 2010).

School IT systems capacity and security will be reviewed regularly.

Security strategies will be discussed with the service provider.

E-mail

Pupils may only use approved e-mail accounts on the school system and are encouraged to use the e-mail account they have within Studywiz.

Pupils must immediately tell a teacher if they receive offensive e-mail (cyber-bullying).

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Headteacher, e-Learning Leader and admin staff will take overall editorial responsibility and ensure that content is accurate and up to date.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

The school will block/filter access to social networking sites (such as Facebook, Twitter etc).

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Staff will not accept parents or pupils as friends on social networking sites.

Managing filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the e-safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is regarded as cyber-bullying and will be dealt with in accordance with the school anti-bullying policy.

Protecting personal data:

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Policy Decisions:

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material (locked down system). However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit IT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Communications Policy:

Introducing the E-safety policy to pupils

Pupils will be informed that network and Internet use will be monitored.

Staff and the e-safety policy

All staff will be given the School e-safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Schools have a major role to play in developing pupils' understanding of how to use new technologies safely. However, pupils spend the greater part of their lives away from school, where the extent to which they are safe and use new technologies responsibly depends on how effectively their families oversee what they do. To ensure continuity of care, it is therefore essential that schools and families work closely together

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school Website.

Staff Support and Training:

- School will audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies.
- All teachers responsible for delivering e-safety education.
- LA to advise on emerging issues and offer training to e-Learning Leader who will in turn disseminate to all staff.

Assessment, monitoring and reviewing:

The teaching of E-safety in lessons covers the following areas:

- Personal details.
- Responding to SPAM e-mail and texts.
- Chat rooms (Years 5 and 6).
- Social Networking sites (Years 5 and 6).

Assessment of the children's learning is achieved through discussion, circle time and role play.

The effectiveness of the e-safety education programme is evaluated by the ethos of the school and the children's behaviour both in the school community and the wider community that they represent. Continual monitoring and evaluation at all levels of representation will help to maintain the success of the programme.

Key priorities for developing an action plan:

- Ensure all staff make pupils aware of the e-safety principles outlined above.
- Ensure continuity and progression throughout key stages.
- Review materials and resources annually so that they are up to date and meet current requirements.
- Share good practice.
- Keep up to date with emerging technologies and potential e-safety issues.

This policy will relates to other school policies including curriculum policy, anti-bullying policy, healthy and safety policy, child protection policy, PSHCE policy and citizenship policy.

A copy of this policy will be given to all employees and will be displayed within the school.