The Mill Academy

E-Safety policy

September 2023

Protecting young people (and adults) properly means thinking beyond the traditional school environment. Where once the desktop computer was the only way to access the internet, now many mobile phones and games consoles offer broadband connections.

Our pupils may be working online in school or at home. They may have personal devices not covered by network protection and therefore the emphasis should be on getting everyone to understand the risks and act accordingly.

This means that designing and implementing e-safety policies demands the involvement of a wide range of interest groups: Headteacher, Governors , senior management , classroom teachers, support staff, young people and parents or carers, Local authority personnel, Internet Service Providers (ISP), Regional broadband consortia, working closely with ISPs on network security measures.

It should already be obvious that e-safety is a child safety, not an Information and Communication Technology (ICT) issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An e-safety policy should:

- allow young people to develop their own protection strategies for when adult supervision and technological protection are not available
- give information on where to seek help and how to report incidents
- help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online
- provide guidelines for parents, carers and others on safe practice
- ensure you regularly monitor and review your policies with stakeholders

- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety program.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

At The Mill Academy, the safety of our children is paramount. This policy is written with that in mind.

Writing and reviewing the e-Safety Policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-Bullying and for Safeguarding.

The school's appointed e-Safety Co-ordinator is currently Miss Crossley, and it should be advised that this is not a technical role.

Our e-Safety Policy has been written by the school, with guidance from other agencies. It has been agreed by staff and approved by governors.

- Adopted by Governors...~~September~~ 12th October 2023.....
- Signed .....Kmylie.....
- Review date: September 2024

1. Teaching and Learning

1.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

- Pupils will be taught how to access appropriate sites
- Pupils will be taught to understand the consequences of inaccurate selection
- Pupils will be taught the procedure to follow should they gain access to an inappropriate site
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.

1.3 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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content to the e-Safety co-ordinator. This will be treated in confidence.

2. Managing Internet Access

2.1 Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be automatically updated regularly.
- Security strategies will be discussed with the Local Authority.

2.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known although this does not guarantee that the e-mail is safe.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Headteacher/Assistant Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

2.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

2.6 Managing filtering

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. The appropriateness of any filtering and monitoring systems are a matter for individual schools and will be informed in part, by the risk assessment required by the Prevent Duty.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

· Identify and assign roles and responsibilities to manage filtering and monitoring systems.

· Review filtering and monitoring provision at least annually.

· Block harmful and inappropriate content without unreasonably impacting teaching and learning.

· Have effective monitoring strategies in place that meet their safeguarding needs Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

St. Mary's Academy Trust has an 'Online Safety Policy' which all schools must follow.

2.8 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff will not use personal mobile phones to communicate with children, or use them to capture images of them.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.9 Protecting personal data

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

3. Policy Decisions

3.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person wishing to access the Internet will be required to agree to the LA 'Acceptable

3.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. 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 computer connected to the school network.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

3.3 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/Assistant Headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures. (See Appendix 2)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- In the cases of any online misconduct, the school Safeguarding Policy will be followed (and Police where appropriate)

3.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

4. Communications Policy

4.1 Introducing the e-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- Safety training will be embedded within the ICT lessons, wider curriculum lessons, RHSE curriculum and our collective worships.

4.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

4.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, social media pages and on the school Web site.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

4.4 Advice for parents

- Use internet filtering software and child friendly search engines. Browser controls often offer differing degrees of security for each family member.
- Check out what safeguarding services your Internet Service Provider (ISP) offers.
- Keep the computer in a communal area of the house.
- Tell your children not to give out any personal details. If they want to subscribe to a service (after gaining your permission) make up a family name.
- Encourage your children to tell you if they feel upset or threatened by what they see online.
- Write a family 'acceptable use policy' for working on the computer.
- Surf together, and be a part of their online life.

(www.cybersentinel.co.uk)

Appendix 1

Activities	Key e-safety issues	Relevant websites Where applicable
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Google
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	
Publishing pupils work on school and other websites.	Pupils' full names and other personal information should be omitted. Pupils work should only be published on „moderated sites" and by the school administrator.	Twitter School web site
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Twitter and School website

Appendix 2 Useful resources for teachers

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents
NSPCC Keeping children safe online
https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Staying safe when you're online
https://www.barnsley.gov.uk/services/training-and-development/digital-skills-and-learning/staying-safe-when-youre-online/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk