



## Online Safety Policy



*At Two Mile Ash school high expectations of learning, behaviour and respect for each other underpin everything we do. Our teachers strive to create independent, articulate thinkers and learners who have the confidence to achieve their ambitions. This drives us in our pursuit for excellence every day.*

## **Online Safety Policy**

### **Philosophy**

At TMA the development of all children's social, moral, spiritual and cultural growth is paramount. We believe that the most important function of the school is to maintain an environment in which every member of the school is able to achieve success and self-fulfilment. There must be a total consistency of expectation that everyone (irrespective of gender, race or culture) should feel safe and secure, have empathy for all others, and place a high value upon individual achievement and personal development.

### **Safeguarding**

At Two Mile Ash School, safeguarding and child protection is paramount and we are fully committed to ensuring the welfare and safety of all our children. We believe that students have a right to learn in a supportive, caring and safe environment which includes the right to protection from all types of abuse; where staff are vigilant for signs of any student in distress and are confident about applying the processes to avert and alleviate any such problems. If any behaviour is a concern in relation to safeguarding TMA procedures and processes will be followed at all times in accordance with the Safeguarding and Child Protection Policy. Any concerns will be referred to the Designated Safeguarding Leads, Hayley Donohue or Lucy Eldridge, Sophie Haycock, Roxanne Jackson, Sally Moisi and Kelly Cursley our Deputy Designated Safeguarding Leads. Our Safeguarding Governor is Nikki Williams.

### **ICT Health, Safety and Welfare.**

The Internet is becoming as commonplace as the telephone or TV in today's society; its effective use is an essential life-skill. The Internet is an essential element in 21<sup>st</sup> Century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Our school has a duty to provide students with quality Internet access as part of their learning experience.

Online safety includes, but is not limited to, browsing the internet. Other forms of electronic communication and interaction such as e-mail, blogging, social networking and online gaming should be considered as well as the corruption, misuse, hacking and publication of personal data.

When using the internet, young people need to be protected from dangers including violence, racism and exploitation. Much of the material on the Internet is published for an adult audience and therefore may be unsuitable for pupils. They need to learn to recognise and avoid any potential risks – to become “Internet Wise”. Pupils need clear guidance in order to prepare them to respond appropriately to any situation, using any of the previously mentioned methods of electronic communication, for the inevitable moment when they come across inappropriate material or find themselves in an uncomfortable situation.

A clear school policy is required to help to ensure the safety of our staff and pupils. We have a requirement to provide pupils with as safe an environment as possible and a need to teach them to be aware of and how to respond responsibly to any of the risks.

- ***Writing, agreement and review of the E-Safety policy.***

Our Online Safety policy has been written by the school using Local Authority and Government advice. It has been agreed by the SMT, SLT and governors. The policy and its implementation will be reviewed annually.

- ***Why the Internet and electronic communication use is important.***

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions.

Internet use forms part of the statutory curriculum and as such is a necessary tool for learning.

The Internet forms part of everyday society and as such it is every schools duty to prepare its pupils through quality Internet access with the personal tools to evaluate information and to take care.

There are benefits to the Internet and planned government initiatives such as:

- Access to world-wide educational resources. (museums or galleries)
  - Inclusion in the National Education Network connecting schools together.
  - The potential for world-wide educational and cultural exchanges.
  - Access to national developments, educational materials and resources to enhance the National Curriculum.
  - Exchange of curriculum and assessment data between National bodies.
  - Access school assessment, curriculum and personal resources from any location that has an internet connection.
  - The facility to extend learning beyond the traditional school building into an electronic environment.
- 
- ***How the internet will be used to enhance learning.***
  - School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
  - All Classes will be taught 'Rules for Responsible Internet Use', at the beginning of a school year, and the skills needed in order to use the Internet appropriately. Children in all classes will sign an agreement to use the internet appropriately and responsibly, as they have been taught to.

- Internet access will be planned to enrich and extend learning activities, and pupils will be given clear objectives for all Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Supervision is the key strategy, aimless surfing should never be allowed – pupils should always use the Internet in response to an articulated need.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT Manager.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using information from the internet.

▪ ***Security of information and systems.***

Online safety will encompass the security of not only the internet but the delivery of internet services and computer applications in school. Issues surrounding the security of access are deemed as important as safeguarding staff and pupils use of on on-line activities.

Staff and pupils will be expected to take responsibility for their use of the network. As part of their daily use they can be reasonably expected to:

- Keep their password secret from peers.
- Ensure that they securely logoff from any workstation they use during the day.
- Act to ensure they speed of the network by selecting the most appropriate time to download large resources or watch on-line TV content.
- Clean up unused files from the network to assist with the longevity of disk storage devices.
- Ensure the removal of any portable storage devices or media.
- Password protect any confidential or sensitive information.
- Not open any attachments, executables or files from unknown or untrusted sources.
- Report any concerns or possible breaches of security to the ICT Development Manager.

- Realise that school ICT space is not personal space.
- Not take copies of any materials that belong to or are the intellectual property of the school.
- To leave copies of any planning or resources, created using ICT, that are required by the school.

The IT Manager will take reasonable steps to ensure:

- Workstations will be configured to prevent user mistakes, deliberate actions or tampering.
- Servers will be located in a locked room with only key personnel given access to room through the use of a key pad entry system.
- Virus protection systems will be provided, secured and kept up to date.
- Access by wireless devices will be strictly controlled and ad-hoc access prevented through the use of authentication protocols.
- The server operating system will be secured and kept up to date.
- All inbound internet connections are configured to prevent unauthorized access.
- Firewalls will be in place to prevent unauthorised access.
- Files held on the school network will be regularly checked for content.
- Monitoring of files and Internet usage will be handled in a professional and discrete way.
- Breaches of protocols will be discussed and acted upon in collaboration with the IT Manager and SLT.
- The IT Manager will review system security and capacity regularly.
- Locally block access to websites or any other content that it deems inappropriate (the blocked list).
- Notify the company providing our internet filtering in the event of any inappropriate materials inadvertently being accessed via the Internet.

- ***E-Mail***

Directed e-mail use can bring significant educational benefits, however the use of e-mail requires that appropriate safety measures are also put into place. At TMA, incoming and outgoing e-mail is limited within the school network for pupils but staff will have external access. All school provided e-mail accounts are filtered and subject to monitoring.

- Pupils may only use approved e-mail accounts on the school system.
- Pupil access to external e-mail addresses is not permitted.
- Staff will be encouraged not to access external e-mail accounts at school. Any access during directed teaching time is strictly forbidden.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as their address or telephone number, or arrange to meet anyone through e-mail communication.
- Whole class or group e-mail addresses should be used when classes wish to contact external organisations or personnel.
- The forwarding of chain letters is banned.
- Official e-mail sent to parents should be written carefully and authorised before sending.
- Staff should ensure all emails sent to professional organisations are professional and courteous.
- 

- ***The management and publication of content.***

In this age, the use of websites to showcase a school and the work it produces has become extremely popular. However, it does provide opportunities acquiring sensitive and personal data if consideration is not given to the material available.

Unlike newspapers, the publication of pupil faces and full names is not acceptable. These published images could be re-used especially if a large image has been used. In addition to this, the publication of names and contact

details of staff will be discouraged and where necessary, access to this information will be available via other methods or through a secure portal.

Only the schools contact details will be published. Staff or pupil contact information will not be published. The Communication Officer and SLT will take editorial responsibility and ensure content is accurate and appropriate. At all times, intellectual property and copyright rights will be respected and complied with.

- Under no circumstances is a pupils' full name to be published anywhere on a website especially when it might relate to a photograph.
- Parents will be given the right to 'opt out' of digital publication in any form of their child on the internet.
- The 'opt out' information will be updated annually and records will be kept.
- At all times, the pupils in photographs should, of course, be appropriately clothed.

- ***Social Networking and personal publishing***

The recent upsurge in the popularity of social networking sites such as Facebook, Snapchat, Instagram and Twitter requires schools to be aware of the potential dangers to staff and pupils. It has become much easier for individuals to publish content and information about themselves on the Internet. The risk of identity theft and the misuse of published photographic material should be considered as risks by all and appropriate steps to educate and protect staff and pupils be made.

- All social networking sites will be blocked in school.
- Consideration will be given, at all times, on how to educate pupils in their safe use.
- Pupils will be advised never to give out information that will identify themselves, their friends or their location.
- Pupils will be directed towards moderated sites.

- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be encouraged not to publish photographic content of themselves.
- Staff should not identify pupils of their place of work in status updates.
- Staff will be advised not to accept requests from current or past pupils.
- Staff must not publish photographic content that contains any images from school or of pupils.
- Staff should not publish status updates regarding school life.

- ***Filtering Internet Content***

In a perfect world, filtering would be 100% accurate and inappropriate material would not be visible to pupils using the Internet. In practice this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable and threatening. Such a procedure will be detailed further into the policy.

- The school will ensure systems are in place to filter website content.
- The IT Manager will make checks to ensure that the filtering is appropriate, effective and reasonable and this is monitored regularly.
- A local school list (The blacklist) will be maintained to further control the websites available within the school.
- A local school list (The whitelist) will be used to temporarily open access to websites for educational use by teaching staff. (All temporary access must be agreed with the technician and strict timings agreed)
- You Tube and other video content websites will be available in school for the use of teachers and support staff. Children are permitted to access You Tube or video content websites at school, but only with permission and supervision by a member of teaching staff.

If for any reason, the filtering blocks a website that a class teacher feels would be of benefit to the children then it can be added to a whitelisted category and therefore be unblocked for teacher/pupil use. Such additions should be made to the IT Manager who will make a decision on whether or not to add the website to the white list.

The school will also regularly monitor the websites that children access. By producing a monthly list of the most visited websites a picture of the usage and activities of the children can be obtained. The list of websites will be reviewed monthly and when appropriate, additional domains and websites may be added to the blocked list.

- ***Videoconferencing and webcams***

The rapid expansion of communications technology requires the school to have a policy on its potential use in education.

- All videoconferences and webcams must make use of the school network to ensure quality of service and security.
- Teachers must request permission from SLT before making a call or using a webcam in a lesson.
- All webcam use will be supervised.
- At no point will any live streaming from school be permitted to be viewed on the Internet or through the school website.

- ***Managing new technologies.***

Small wireless devices provide more opportunities for pupils to be exposed to content within school that cannot be controlled or filtered through the school network or security systems. This can even extend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people. At all times we need to be aware of the current technology and its possible risk and educational benefit.

- Pupils' mobile phones will be permitted in school for safety reasons but they should be switched off during school hours and not be used within the school grounds.
- The use of cameras in mobile phones is not permitted.
- A blog may only be used in school by pupils if it is appropriately moderated.
- The school will ensure its network will block connections from devices that are not part of its domain. (Personal laptops, iPads, iPod touches, wireless mobiles)
- The use of 3G broadband devices is not permitted as it will bypass all school filtering systems.

- ***Protection of personal data***

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

- ***Authorisation of Internet access***

Staff need to be vigilant and ensure that any use of the Internet by pupils must be authorised and supervised at all times. This will ensure that any potential risks are reduced and that a pupil will have an immediate point of contact should they have a problem or are uncertain of about a course of action to take.

All staff and pupils must be made aware of the rules and regulations surrounding the use of any ICT resource before beginning to use it in education.

- All staff will ensure that they have read and signed a 'staff code of conduct for ICT'
- All pupils will be taught about internet safety and will sign a 'class agreement'

- At all times a record of staff and pupils who are granted access to the school network will be maintained.
- Any person not employed by the school must be made aware of the rules and acceptable use of ICT systems before being allowed access.

- ***Risk management***

At all times staff, pupils and parents should be made aware that;

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 cannot accept liability for any material accessed, or any consequences of Internet access.

Regular audits of ICT use will establish if the e-safety policy is adequate and that the implementation of the policy is appropriate and effective.

***Online Safety complaints.***

- Staff misuse will be referred to the Headteacher
- Complaints made about Internet misuse will be dealt with by the IT manager and SLT.
- Complaints of a child protection nature must be dealt with in line with the school child protection procedures.
- Parents and pupils will be informed of any necessary complaints procedure.
- Parents, pupils and staff will be made aware of the consequences of the misuse of the Internet or school resources.

- ***Regulation***

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. Fair rules, prominently displayed will help pupils to make responsible decisions.

- Rules for Internet access and E-mail use will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede all Internet and E-Mail access.
- Staff will be made aware of their responsibilities through the distribution of the online safety policy.
- Staff will be informed that Internet use can be monitored.
- Monitoring will be carried out by the IT Manager working to clear procedures for reporting issues.
- Parents/carers will be made aware of the schools online safety policies.

- ***Abuse of the System***

Any transgressions of the rules which are minor can be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and sanctions available include:

- An interview/counselling by YGM/Head of Year;
- Informing parents or carers;
- The Removal of Internet or computer access for a set period of time.

## Two Mile Ash School

### Staff ICT Code of Conduct

- I will ensure that I keep my password safe.
- I will ensure that I securely logoff from any workstation I use during the day.
- I will safeguard the speed of the network by selecting the most appropriate time to download large resources or watch on-line TV content.
- I will clean up unused files from the network to assist with the longevity of disk storage devices.
- I will ensure I remove any portable storage devices or media that I use in the school computers
- I will password protect any confidential or sensitive information that I store on portable storage devices.
- I will not open any attachments, executables or files from unknown or untrusted sources.
- I realise that school ICT space is not personal space.
- I will not take copies of any materials that belong to or are the intellectual property of the school.
- I will leave copies of any planning or resources, created using ICT, that are required by the school.
- I will not use the school ICT equipment for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will not to reveal personal information about the pupils I teach or the school through email, personal publishing, blogs or messaging.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will report any incidents of concern regarding children's safety to the IT Manager, the Designated Safeguarding Lead or SLT.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system

may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read and understand the rules of ICT use.

Signed : \_\_\_\_\_

Date: \_\_\_\_\_

Pupils ICT Rules  
Class \_\_\_\_\_

These rules help us to stay safe on the Internet



- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.



- We immediately close any webpage we not sure about.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.



- We do not use Internet chat rooms
- We do not use You Tube or other video websites in school.
- We the undersigned agree to these rules.

