

INTERNET SAFETY POLICY

Introduction and Aims

The aim of this policy is to create a safe ICT learning environment. This will be achieved by;

- an infrastructure of whole-site awareness, responsibilities, policies and procedures
- an effective range of technological tools
- a comprehensive internet safety education programme for pupils, staff and parents
- a review process continually to monitor effectiveness and keep pace with new technology

Queen Mary's believes that internet safety involves school and home and that it is a shared responsibility.

Method

To achieve our aims Queens Mary's has:

- Developed an *Acceptable Use Policy* (AUP) detailing the ways staff, pupils and all network users can and cannot use the ICT facilities.
- Used monitoring, virus protection and firewall software.
- Designated a senior management team member (Paul Nuttall) to be the central contact point for all internet safety issues.
- Implemented an education programme to make pupils, staff and parents aware of potential risks and how to practise safe, responsible behaviour whenever they are online.
- Agreed to review the policy at regular intervals.

The underlying goal is to allow pupils to develop their own protection strategies by:

- giving information on where to seek help and how to report incidents
- outlining sanctions that will be taken if they act inappropriately when online
- providing guidelines for parents on safe practice
- educating pupils about the risks
- clear explanation of the Acceptable Use Policy

Use of Technology in Safeguarding

Software is used to provide the following safeguards, protection and boundaries:

- Filtering – user defined groups have an increased level of internet site accessibility. These groups are:

Years 1 and 2

Years 3 to 6
Years 7 and 8
S1 to S3

Details of the sites available to each group are attached.

- Time limits for internet access – 10 p.m. no access for any pupil until 7 a.m.

Years 1 and 2	8.30 a.m. to 4.10 p.m.
Years 3 to 6	7.00 a.m. to 8.00 p.m.
Years 7 and 8	7.00 a.m. to 9.00 p.m.
S1 to S3	7.00 a.m. to 10.00 p.m.

- Email addresses – must be via school webmail. All others will be blocked
- Virus protection
- Logging – views of excessive use of internet and particular sites. Use to educate about time wasting etc

Acceptable Use Policy

The aim of this AUP is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed.

General:

- Users are encouraged to make use of the school's computing facilities for educational purposes.
- All users are expected to act responsibly and show consideration to others.
- Users can access the school intranet from outside school via the school's website using their user login and password.
- Users should not divulge their password to anybody.
- Users should not logon to or use any account other than their own and should logoff when leaving a workstation, even for just a short period of time.
- Users should be aware that the school filters the internet service to prevent access to inappropriate content.
- In the event of any improper content getting past the filtering system users must inform a member of staff immediately
- Users should be aware that the school logs all internet use.

It is not acceptable to:

- Attempt to download, store or install software to school computers.
- Attempt to introduce a virus to the network.
- Attempt to bypass the system's security and filters.
- Attempt to access another user's account.
- Attempt to use any form of cracking software.

- Access the internet via a connection not provided by the school.
- Access, download, create, store or transmit material that is indecent, obscene, offensive or causes annoyance or anxiety to others.
- Infringe copyrights.
- Access, download, create, store or transmit material that brings the school into disrepute.

Chat rooms:

- These sites are banned

Instant messaging:

e.g. msn, yahoo messenger

- These are allowed at lunch time between 1.10 p.m. and 2.10 p.m. and in the evening between 4.30 p.m. and 6.30 p.m.
- Only personally known contacts are to be added to the list of contacts.

Email:

Pupils must

- Not use email during lessons.
- Not open email or attachments from an unknown sender.
- Report offensive, upsetting and anonymous emails to Mr Nuttall.
- Not send or forward chain emails.
- Only use email facilities provided by school – others will be blocked.

Social Networking:

e.g. Facebook, Bebo,

- Not legal for people under 13 years old
- Only users in the S1 to S3 user group are allowed access
- Time limits as follows:
lunch time between 1.10 p.m. and 2.10 p.m. and
in the evening between 4.30 p.m. and 6.30 p.m.
- No photographs or information about other people must be added without their written consent.
- All personal details must be kept private.

Laptops:

- Only to be used in Year 7 and above
- Must be given to Mr Vivian to enable access to the internet via the school network.
- Must have antivirus protection installed.
- Use is a privilege, not a right. Misuse will lose the privilege.

Personal Safety:

- Pupils should take advantage of the education programme provided.
- Respect the privacy of others.
- Look after the welfare of others.
- Report worries they might have about others' use of the internet.

- Pupils should not supply personal information about themselves or others via the web, email or social networking sites.
- Pupils must never attempt to or arrange meetings with anyone met via the web, email or social networking sites.
- Pupils must realise that the school has access to their personal areas on the network. Privacy will be respected unless there is reason to believe that the Acceptable Use Policy or school guidelines are not being followed.

Sanctions:

It is hoped that pupils will have respect for themselves and for others in their use of the ICT facilities and in particular the internet. The school has a duty to safeguard pupils and will take steps to do so. Education about usage and safety are the primary means of ensuring acceptable use of the system. However, misuse of the facilities and not following the Acceptable Use Policy will result in disciplinary procedures.

Internet Safety Education Programme

Queen Mary's believes that the key to internet safety lies in an effective education programme for pupils, staff and parents.

Issues of safety will be taught to pupils in ICT lessons and during PSHE sessions. The CEOP, Thinkuknow and Kidsmart resources provide a basis for education.

An information evening for parents will also be arranged if interest is shown.

Topics to be addressed:

- Safe emailing
- Social networking sites
- Cyberbullying
- Copyright and plagiarism
- Chat rooms and Instant Messaging
- Acceptable Use Policy
- Virus protection

Group Filtering

Smooth Wall operates by using URL filtering categories. Within each main category are sub categories to allow a more specific filter to be applied. Queen Mary's have allowed increased access to the available categories as pupils go up the age defined groups outlined in the policy. These groups are:

- Years 1 and 2
- Years 3 to 6
- Years 7 and 8
- S1 to S3

The following categories are available to all groups:

- Good Content – e.g. email, news, windows updates
- Search engines
- User defined – e.g. sites requested specifically by staff

The following categories are filtered from all groups with certain exceptions:

- Adult themes – except Illegal and Legal drugs for S1 to S3 to allow research
- Bad Language
- Computer games, Web based games and Desktop Sillies
- Malware and hacking
- Medical – except for S1 to S3 to allow research
- Audio video and Peer-to-peer networking
- Pornography keywords
- Chat rooms and dating sites
- Instant messaging sites
- Social networking sites – except for S1 to S3 in their specified times
- Ringtones and vacations
- Adverts
- E-Commerce
- Intolerance
- Online auctions
- Personal finance
- Pornography
- School cheating
- Webmail