Queen Mary's Grammar School

A statement of our policy on

E-Safety

Approved by the Local Governing Board, November 2017

1. Rationale

ICT is a vital part of teaching and learning in the School community and is a crucial tool for staff and students alike. It also has an integral role in the School's management information and business administration systems. Access to the Internet is an essential tool for all staff and a privilege for students.

The e-Safety Policy is important in school for a number of reasons, including the following:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for students is aware of his/her responsibilities.
- To set boundaries of use (goalposts) of any school owned ICT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. Twitter).

2. Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, members of the governing body, School volunteers, students and any other person working in or on behalf of the School, including contractors who use any of the School's ICT equipment or facilities.

Parent – any adult with a legal responsibility for the child/young person outside the School e.g. parent, guardian, carer.

School – includes any school business or activity conducted on or off the School site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, members of the governing body, parents.

Safeguarding is a serious matter; technology and the Internet are used extensively at the School across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The two overriding purposes of this policy are:

- To enable the whole School community to stay as safe and risk free as possible;
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce the possibility of harm to the student or liability to the School.

This policy is available on the QMGS website.

Following approval by the Governing Body and after any review:

- Users (including staff) must sign the Computer Network User Agreement at Appendix 3 to confirm they have read and understood both the e-safety policy and the School Computer Network User Terms and Conditions at Appendix 2 ("the Terms and Conditions".).
- Students will be permitted access to the School's technology (including the Internet) only when they have returned the signed and countersigned Computer Network Student User Agreement (Appendix 6) and the Acceptable Use Agreements (Appendix 4/5) that will be distributed at the beginning of each key stage (years 7, 10 and 12).

3. Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is responsible for ensuring that the School has effective policies and procedures in place; as such it will:

- Review this policy at least annually and in response to all e-safety incidents:
  - to ensure that the policy takes into account the evolution of e-Safety and its position in the school,
  - covers all aspects of technology use within the School,
  - to ensure e-safety incidents were appropriately dealt with and that the policy was effective in managing those incidents.

- Appoint one governor (the "Responsible Governor") to have overall responsibility for the governance of e-safety at the School and who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headmaster in regards to training, identified risks and any incidents.

Head of School

Reporting to the governing body, the Head of School has overall responsibility for e-safety within the School. The day-to-day management of this will be delegated to the e-Safety Adviser, as indicated below.

The Head of School will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body, and parents.
- The designated e-Safety Adviser has had appropriate training in order to undertake the day to day duties.

- All e-Safety incidents are dealt with promptly and appropriately.

Assistant Head/Designated Safeguarding Lead

The Assistant Head (who also acts as the Designated Safeguarding Lead) will:

- Be the first point of call for e-Safety related discipline issues
- To liaise with the IT Network Manager and e-Safety Adviser to follow up issues and arrange appropriate sanctions
- To support Heads of Year in delivering e-Safety awareness material

e-Safety Adviser

The e-Safety Adviser will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters of concern to the attention of the Head of school
- Advise the Head of school and governing body on e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, ICT technical support and other agencies as required.
- To liaise with the IT Network Manager to ensure any technical e-safety measures in school (e.g. Internet filtering software, and behaviour management software) are fit for purpose
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Head of school and responsible governor to decide on what reports may be appropriate
- Be familiar with any reporting function regarding e-safety measures, including internet filtering, and review appropriate reports with the Headmaster and the Responsible Governor to ensure compliance with this Policy.

Network Manager

The Network Manager is responsible for ensuring that:

- The ICT technical infrastructure is maintained; this will include as a minimum ensuring that:
    - Anti-virus protection is fit-for-purpose, up to date and applied to all capable devices.
    - All operating systems/system updates are regularly monitored and devices updated as appropriate.
    - Any e-safety measures such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety adviser and Head of school
    - Passwords are applied to all users regardless of age.
- For security reasons, the IT System Administrator account is to be used only for the purposes of system administration rather than day-to-day tasks. Third parties (i.e. engineers, contractors) requiring this level of access shall be provided with a separate account with appropriate privileges unless

administrator access is absolutely necessary. This account shall then be removed or disabled on completion of said task at the Network Managers discretion.
- The primary server is properly functioning except during maintenance or rebooting, including school holiday periods.
- Any personal data or software is removed from the PC/laptop if the individual is not authorised to receive the data.
- Care is taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.
- Any personal data or software is removed from the PC/laptop if the individual is not authorised to receive the data.
- Care is taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

All Staff

Staff must ensure that:
- They read and understand the Terms and Conditions (along with the Social Media Policy);, and sign the Computer Network User Agreement. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Staff Conduct Policy.
- A regular audit of the e-Safety training needs of all staff is carried out.
- All new staff receive e-Safety training as part of their induction programme.
- All actions must comply with the legislation, including the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.
- Any e-safety incident is reported to either the e-Safety Adviser or Assistant Head or, in their absence to the Head of School. If in doubt the matter is to be raised with the e-Safety Adviser or the Head of School to make a decision. In exceptional circumstances, an e-safety incident may be reported directly to the Chair of Governors.

All Students

For students, the use of ICT equipment and services in this school is a privilege and not a right. Before they are permitted access, students must:
- At the start of each key stage (years 7, 9, 12), read and understand the Terms and Conditions in Appendix 2, and sign and have countersigned by a parent the Computer Network Student User Agreement contained in Appendix 6, and the Acceptable Use Agreements at Appendix 4/5.
- Understand that any deviation or misuse of ICT equipment or services will be dealt with in accordance with the School's Behaviour Policy.

E-Safety is embedded into the curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be made aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will use its best endeavours to keep parents up to date with new and emerging safety risks, and involve parents in strategies to ensure that students are made aware of such risks. Through parents evenings, school newsletters, information on the website, end of term packs, the School will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand that the School needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will countersign the Computer Network Student User Agreement before any access can be granted to school ICT equipment or services for their son/daughter.

Senior Leadership Team

The SLT is responsible for:

- advising on changes to the e-Safety policy;
- establishing the effectiveness of e-Safety training and awareness in the school;
- recommending further initiatives for e-Safety training and awareness at the school.
- Present the e-Safety Policy for annual review to the governing body

4. Technology

The School uses a range of devices including PCs, Laptops, Tablets and Smart-Phones. In order to safeguard students and in order to prevent loss of personal data the school employs the following technology:

(i) **Internet Filtering** - prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; what is "inappropriate" will be determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Network Manager (in conjunction with the School's internet provider) is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School.

(ii) **Email Filtering** - software that helps preventany spam or infected email being sent or received by the school. Infected is defined as: an email that contains a virus or malicious script (i.e. malware) that could be damaging or destructive to data.~~; spam email such as a phishing message.~~

(iii) **Passwords** all staff and students must access devices using their unique username and password. Staff and students are advised to change their passwords on a termly basis and must do so if their account has been compromised or following on from an e-Safety incident. All school devices that hold personal data (as defined by the Data Protection Act 1998)

should be password protected. No data is to leave the school on an unprotected device~~; all devices that are kept on school property and which may contain personal data are protected~~. Any breach (e.g. loss/theft of devices such as: laptops or USB key drives, or unauthorised access to:mark books, SIMS orAIM HIGH from home) is to be brought to the attention of the Head of School immediately. The Head of School will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

(iv) **Anti-Virus** – All school devices must have anti-virus software. The School's system is updated daily for new virus definitions. ICT Support will be responsible for ensuring this task is carried out, and will report to the Head of School if there are any concerns. All USB peripherals such as key drives must be scanned for viruses before use. The same anti-virus software is used throughout all school owned devices.

5. Mobile phones and other BYODs (Bring Your Own Devices)

The School recognises that mobile phones play a significant role in the life of most pupils and that they can have considerable value in relation to individual safety. It is not in pupils' or families' best interests to prohibit phones from being brought into school, nor is it logistically possible to collect them in the morning and return them at 4pm. The School therefore permits pupils to bring mobile phones into school, but that permission is subject to certain limitations.

School use of mobile devices, including laptops, tablets and mobile phones is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of e-Safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

It must be understood that should handheld devices be misused, there may be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones and handheld devices can also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. For this reason, devices should not be used unless directed by a member of staff between the hours of 9am and 4pm. They should not be used in

public places during these times – i.e. the canteen, corridors, classrooms and reception area. Sixth form students may use devices in the Bateman room.

All users must understand that whenever they connect a device to the school's network the opportunity exists for:

- Introducing viruses, spyware, or other malware.
- Purposefully or inadvertently copying sensitive and/or proprietary school information to unauthorized devices.
- Introducing a technical or network incompatibility to the school that the user is not even aware of.
- As a result of any of these three circumstances, a user connecting his or her own device to school resources, systems, or networks could interrupt school continuity, cause unplanned downtime for multiple users, and/or cause a data breach releasing sensitive school data to unauthorized parties.

Guidelines on the use of personal devices

- Mobile devices brought into school are entirely at the staff member, student, parents or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school. It is the responsibility of parents and pupils to ensure that phones are properly insured, and kept safe during the day. They must be stored in lockers unless required (by a teacher) for use in lessons
- The recording, taking and sharing of images, video and audio on any mobile device is to be avoided; except where it has been explicitly agreed otherwise by the Head of school. Such authorised use is to be monitored and recorded. All mobile device use is to be open to scrutiny and the Head of School is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Access to the School's wireless internet network must be through the appropriate password enabled route and will be open to the same scrutiny as with the use of school devices. Misuse of this privilege will result in disciplinary procedures in accordance with the 'Discipline Policy'
- Mobile devices are not allowed in examination rooms, along with smart watches. They must be left in a locker or handed in to the invigilator.

Pupil safety

- All pupils must ensure that files stored on their devices do not contain violent, degrading or pornographic images. The transmission of some information is a criminal offence. Pupils who are found to be in breach of this rule can expect to have their phone confiscated; it will be returned to their parents, or in extreme cases passed to the police.
- Cyber-bullying is completely unacceptable and will not be tolerated in our school community. Pupils who are found to have used their phones for this purpose can expect to have their phone confiscated and to be severely punished.

Emergencies

- If a pupil needs to contact his or her parents, he or she should report to the School Office, where they will be allowed to use a phone. Pupils must not phone home and arrange to be collected if ill. All calls of this nature must be made through the school office.
- If parents need to contact children urgently, they should phone the School Office (01922 720696) and a message will be promptly relayed.
- In exceptional circumstances, pupils will be given permission by a member of staff to use their mobile phone.

Sanctions

- If a pupil is found to be in breach of rules in this policy, the phone will be confiscated and, if in Year 7-11 given to Mr Saran or, in Year 12 and 13, to Mr Matley. It will generally be returned to the pupils at 4pm. Sixth Formers who offend and who would normally sign out will remain in Private Study until 4pm and then collect their phone.
- Persistent offenders will be punished appropriately and their phones retained until collected by parents.

6. Computer Security

Physical security

- Any laptop that is left unattended in a classroom/office must be secured using the appropriate security cable, locked in a cabinet, or the door locked.
- Staff users should ensure that they have logged out of the school network or switched user to 'lock this computer' if they are leaving their laptop unattended during break, lunch or PPA periods.
- Student users should log out of their machine when they leave it unattended
- As far as is practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Appropriate arrangements must be made for the removal of any ICT equipment from its normal location (not including laptops). These arrangements should take into account the risks associated with the removal and the impact these risks might have. Before any ICT equipment (other than laptops) is moved from its normal position, a full risk assessment will be undertaken and recorded by the Network Manager.
- An inventory of school hardware and software must be maintained by the IT Network Manager

- Personal or sensitive data must not be left on monitors, whiteboards, desks or printers so as to be viewable by others.
- Personal or sensitive data should not be stored on USB flash drives or other portable media.
- Users should use their school e-mail account for all school business.
- Personal or sensitive data, both paper and electronic, should be disposed of in a responsible way e.g. shredding of paper copies and deletion of electronic copies.
- All loss or theft of ICT equipment should be reported to the Headmaster

Systems security

- Users must not make, distribute or use unlicensed software or data.
- Users must not make or send threatening, offensive or harassing messages.
- Users must not create, possess or distribute obscene material.
- Ideally, passwords should be alphanumeric and be made up of at least 8 characters
- Users must not share their passwords with any other user.
- Password should not be easily guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords must be changed if affected by a suspected or actual breach of security or other e-safety incident.
- Regular backups of data must be performed by the Network Manager or the ICT support staff.
- Security backups must be tested to ensure that they enable data restoration in the case of systems failure.
- Where possible, security copies should be clearly marked and stored in a fireproof location and/or off site.
- Staff should only allow their laptop to be used by students while they are available to supervise this work.

Virus protection

- Users who wish to continue to use the school's ICT equipment or facilities should connect to the network weekly to ensure that up to date virus protection can be accessed.
- All suspected or actual virus infection must be reported to the e-Safety Adviser or the Network Manager.

E-Safety Incidents

All suspected or actual breaches of information or ICT security, including detection of computer viruses, must be reported to the Network Manager immediately.

7. Safe Use

Internet – Although the use of the Internet is an essential tool for staff, and a privilege for students, access to the Internet will be granted:

- To staff upon signing the School Computer Network User Agreement (see Appendix 3);
- To students when they have returned the Computer Network Students User Agreement which they have signed to indicate they have read and accept the

Terms and Conditions, and which has been countersigned by a parent giving consent.

Email – All staff are reminded that emails are subject to Freedom of Information Act requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address.

Photos and videos – All parents must sign a photo/video release slip at the beginning of the academic year to give consent for the use of photos and videos in accordance with the Policy; non-return of the permission slip will not be assumed as consent.

Social Networking – there are many social networking services available; the School recognises the potential of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Twitter is permitted for use within the school in accordance with the Social Media Policy. No other social media should be used.

In addition, the following are to be strictly adhered to:

- Permission slips (via the school's Photographic Policy) must be obtained before any image or video of any child is uploaded.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day by the IT support team.

Incidents - Any e-Safety incident must be brought to the attention of the Pastoral assistant Head or e-Safety Adviser, or in their absence the Head of school. The Pastoral assistant Head will advise the appropriate action to take.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, the school will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the school; all staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning (e.g. FFP, PSHE, School and Year assemblies)

As well as the programme of training the school will establish further training or lessons as necessary in response to any incidents.

The e-Safety Adviser is responsible for recommending a programme of training and awareness for the school year to the Headmaster and SLT for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headmaster for further CPD.

8. The use of devices as learning support and in examinations

Taken from JCQ 2017-18: Instructions for conducting examinations

The School is allowed to provide a word processor (e.g. laptop, computer) with the spelling and grammar check/predictive text disabled to a candidate where it is their normal way of working within the school, unless an awarding body's specification says otherwise. This also includes an electronic brailler or a tablet.

A word processor:
· must be used as a type-writer, not as a database, although standard formatting software is acceptable;
· must have been cleared of any previously stored data, as must any portable storage medium used. An unauthorised memory stick must not be used by a candidate. Where required, the centre must provide a memory stick to the candidate, which is cleared of any previously stored data;
· must be in good working order at the time of the examination;
· must be accommodated in such a way that other candidates are not disturbed and cannot read the screen. Where a candidate using a word processor is accommodated in another room, a separate invigilator will be required;
· must either be connected to a printer so that a script can be printed off, or have the facility to print from a portable storage medium. This must be done after the examination is over. The candidate must be present to verify that the work printed is his or her own. Word processed scripts must be attached to any answer booklet which contains some of the answers;
· must be used to produce scripts under secure conditions, otherwise they may be refused;
· must not be used to perform skills which are being assessed;
· must not be connected to an intranet or any other means of communication;
· must not give the candidate access to other applications such as a calculator (where prohibited in the examination), spreadsheets etc;
· must not include graphic packages or computer aided design software unless permission has been given to use these;
· must not have any predictive text software or an automatic spelling and grammar check enabled unless the candidate has been permitted a scribe or is using speech recognition technology (a scribe cover sheet must be completed), or the awarding body's specification permits the use of automatic spell checking;
· must not include speech recognition technology unless the candidate has permission to use a scribe or relevant software;
· must not be used on the candidate's

Controlled assessment or coursework components can normally be completed on word processors unless prohibited by the specification.

Principally, that a word processor cannot simply be granted to a candidate because he/she prefers to type rather than write or can work faster on a keyboard, or because he/she uses a laptop at home.

The use of a word processor must reflect the candidate's normal way of working within the centre and be appropriate to the candidate's needs.

The School will arrange for candidates to be assessed through the Special Educational Needs team if it is deemed that a student requires a word processor in an examination. For students who, through an objective testing process, are deemed in need of such a device, the School will make this available.

9. The e-Safety Training Programme 2017-18

	Pupils	Staff	Parents	Other
Autumn Term	Computer Network Agreement Whole School Assembly HoY Assembly FFP	Computer Network Agreement Online monthly school newsletter subscription New Staff, PGCE, Basic e-Safety	Computer Network Agreement HoYs- Online monthly parental newsletter subscription Parents' Evenings End of term pack reminds to check the website	Feeds on Twitter QMGS Website e-Safety tab
Spring Term	E-safety awareness week and Safer Internet day HoY Assembly FFP/PSHEE	INSET Training All Staff-in house/ outside speaker	Parents' Evenings	Feeds on Twitter QMGS Website e-Safety tab Review e-Safety Policy
Summer Term	HoY Assembly FFP/PSHE Pupils Audit	Staff Audit	Parents' Evenings	Feeds on Twitter QMGS Website e-Safety tab

The policy will be reviewed annually by:

- The SLT
- The Pastoral and Curriculum Committee
- Reviewed November 2017

The Network Manager and designated person with responsibility for Computer Security is: Mr. P. Scandrett

The e-Safety Adviser is: Mrs Frances Round

The Designated Safeguarding Lead (DSL) is Mr R. Saran

The Responsible Governor for e-Safety is the Chair of the Pastoral and Curriculum Committee: Mrs. Bonner

Appendices:

1 e-Safety Year Plan
2 School Computer Network User Terms and Conditions
3 School Computer Network User Agreement
4 Students Acceptable Use Agreement (Years 7-9)
5 Students Acceptable Use Agreement (Year 10-13)
6 Computer Network Student/Parent User Agreement
7 Pupils' Online e-Safety Survey

Appendix 1

E-Safety Year Plan

On-going:

- Feeds on Twitter (e.g. join on Twitter @esafetyadviser, @childnet)
- Posters throughout the school
-
- Parents' Evening e-Safety presentation element, leaflet and info on the website
- QMGS Website e-Safety tab
    - Online monthly newsletter
    - Button on the website to report (i.e. CEOP)
    - Attach downloadable files, link to relevant sites, videos etc
    - 'How to' guides

HoY Assembly ideas:

- Plagiarism/Copyright
- Privacy settings on Facebook, Twitter
- Phishing, Phishy Signs
- Identity theft
- Grooming

FFP/PSHE ideas:

- All KS-1st lesson- Student Acceptable Use Policy to be signed and discussed
- Watch a CEOP video and have a discussion (age-relevant)
- Your digital footprint (link it with the relevant current news) - Online Reputation Checklist.pdf
- So you got naked online…- sexting

English & Drama:

- Write a poem on e-Safety topic (e.g. cyber bullying)
- Laugh at it, you're part of it (KS4&5) 5x50min lessons
- Picture This (KS4&5) 5X60min
- Online Rights and Responsibilities: It's our time to be heard! (KS3&4) - This is an open-ended activity that can take as little / as long as is required

Parents' Eve:

- Pocket size e-Safety leaflet
- 'How to' Guides

Sites to visit regularly:

- http://ceop.police.uk/
- http://www.thinkuknow.co.uk/
- http://www.childnet.com/
- http://www.digizen.org/
- http://www.kidscape.org.uk/
- http://www.teachtoday.eu/
- http://www.vodafone.com/content/index/parents/about_digital_parenting.html
- http://www.parentport.org.uk/
- http://www.saferinternet.org.uk/
- http://www.theparentzone.co.uk/
- http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls - How to set up the parental controls offered by your internet provider

Appendix 2

Queen Mary's Grammar School, Walsall.

School Computer Network User Terms and Conditions

Teachers, pupils, students and all other users are required to follow all the conditions laid down in these terms and conditions. Any breach of these conditions may lead to withdrawal of the user's access to the QMGS Computer Network and in some instances could lead to criminal prosecution. In the case of employees, any breach may be considered a breach of the employee's conditions of service, which could lead to dismissal on grounds of gross misconduct.

All users are expected to demonstrate a responsible approach to the use of resources available to them and to show consideration for other users both locally and with whom they may come into contact on the Internet.

Use of the Internet and facilities such as electronic mail services are intended for educational or professional purposes only. It must be demonstrated that any opinion communicated over the Internet is deemed to be that of the author and not that of the School or Governors.

Any use of School computer equipment to access the Internet other than from school premises requires the express permission of the Network Manager.

Subject to the section below on acceptable use, the school equipment and the Internet may only be used for any legal activity consistent with the aims, objectives and rules of the school.

All network users should be aware that user accounts are monitored; all files, electronic mail and web browsing history cannot be deemed private, and may be subject to Freedom of Information Act requests.

UNACCEPTABLE USE

The following activities, whilst not an exhaustive list, are unacceptable:

1. Access to or creation, transmission or publication of any offensive, obscene or indecent messages, images, sounds, data or other material.
2. The creation, transmission or publication of any material that is designed or is likely to cause offence, inconvenience or needless anxiety. Any acts considered by the school to be cyber bullying will be dealt with as a serious disciplinary matter whether undertaken in or outside of school.
3. The creation, transmission or publication of defamatory or discriminatory material.
4. The receipt or transmission of material such that this material infringes current legislation, including copyright and the Data Protection Act 1998
5. The transmission of unsolicited commercial information or advertising, within QMGS Extranet, to users of the Internet or any other computer/network system reachable via the Extranet.
6. The deliberate unauthorised access to facilities, services, data or resources within the QMGS Intranet or any other network or service accessible via the Extranet.
7. Divulging an individual's password to another network user or the use of another user's account at any time.
8. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the QMGS Network and associated resources.
9. Any use of the Internet that would bring the name of the School into disrepute.
10. Deliberate Activities with any of the following characteristics or that by their nature would result in:
    - Wasting staff or other users' time or network resources, including time on remote systems and the time of staff involved in the support of those systems.
    - corrupting or destroying other users' data.
    - violating the privacy of other users.
    - disrupting the work of other users.
    - using the Extranet/Internet in any way that denies services to other users (e.g. by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading or uploading large files).
    - continuing to use any item of software after being requested to cease its use because it is disrupting the correct function of the School's network or the Internet (for example, utilities designed to broadcast network-wide messages, etc.).
    - introduction of any malware (e.g. viruses, worms etc.)
    - e-mails spam/spoofing.
10. Damage to any computer hardware. The school reserves the right to charge for acts of willful vandalism. Use of the School's personal computers (including portables) to access the Internet through an unofficial or unauthorised route.
11. Printing of non-essential material and failure to check that the length of a document is reasonable before printing.
12. Unauthorised wireless access to the school Network.
13. Any other use deemed to be unacceptable by the designated person.

Appendix 3

Queen Mary's Grammar School

School Computer Network User Agreement

Name	

Queen Mary's Grammar School is pleased to offer users access to the Internet and electronic Mail (e-mail) via the School's computer Network, subject to compliance with the School's Computer Network User Terms and Conditions and the e-Safety Policy.

Any deliberate or accidental breaches of the above named Terms and Conditions and policy must be reported immediately to the e-Safety Officer or to the Network Manager...

The e-Safety Officer is Mr. N. Canning, and the Network Manager is Mr. P. Scandrett, and they may be contacted for further information.

User Agreement

I understand that if I deliberately contravene the School's Computer Network User Terms and Condition or the e-Safety Policy, I may lose the opportunity to use the equipment or facilities.

Further, if I am an employee of the School, I recognize that contravention of the Terms and Conditions or the e-Safety policy may result in disciplinary proceedings being taken against me.

As a user of the School's network, I hereby agree to comply with the requirements of the School's Computer Network User Terms and Conditions and e-Safety Policy and any other conditions that the School may from time to time, deem necessary.

Signature	
Job title	
Date	

Appendix 4

Students Acceptable Use Agreement (Year 7-9)

Note: All Internet and email activity is subject to monitoring

Please read and sign the agreement below *(at the beginning of each academic year, in the planner).*

I have read and understood the school Computer Network User Terms and Conditions, and the e-Safety policy. I will use the computer system and internet in a responsible way and obey these rules at all times:

I will only use my own login and password, and I will keep my password a secret. I will change my password at least each term.

I will always lock my computer when unattended and log off when I have finished using it.

I will only use the computers for educational purposes.

I will only email people I know or with my teacher's approval.

My emails **will** be polite and sensible.

I will not show other people's things that may be upsetting.

I will not use other people's work or pictures without permission to do so.

I will not give out any personal information, such as my mobile number or address, or arrange to meet anyone I don't know.

I will not do anything on the Internet that would bring the name of the School or information into disrepute.

I will not damage or rearrange the hardware, or install any software.

I will be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand that some people on the Internet are not who they say they are, and some people can be nasty. I will tell a teacher if I am ever concerned in school, or my parents if I am at home.

I will use the correct password enabled route to access the School's Wi-fi system through my own devices and understand that the same principles of internet use apply as through the use of school equipment

I understand if I break the rules in this Policy. I will be punished in accordance with the School Discipline Policy, my parents will be told and I may lose the privileged use of the equipment.

Name			
Signature			
Form		Date	

Appendix 5

Students Acceptable Use Agreement (Year 10-13)

Note: All Internet and email activity is subject to monitoring

Please read and sign the policy below *(at the beginning of each academic year, in the planner).*

I have read and understood the school Acceptable Use Policy. I will use the computer system and internet in a responsible way. The following activities, whilst not an exhaustive list, are unacceptable:

1. Access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material.
2. The creation, transmission or publication of any material that is designed, or likely, to cause offence, inconvenience or needless anxiety. Any acts considered by the school to be cyber bullying will be dealt with as a serious disciplinary matter whether undertaken in or outside of school.
3. The creation, transmission or publication of defamatory or discriminatory material.
4. The receipt or transmission of material such that this material infringes: the copyright of another person, the conditions of the Data Protection Act 1998 or any other UK laws
5. The transmission of unsolicited commercial information or advertising, within QMGS Extranet, to users of the Internet or any other computer/network system reachable via the Extranet.
6. The deliberate unauthorised access to facilities, services, data or resources within the QMGS Intranet or any other network or service accessible via the Extranet.
7. The divulging of an individual's password to another network user or the use of another user's account at any time.
8. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the QMGS Network and associated resources.
9. Any use of the Internet that would bring the name of the School into disrepute.
10. Logging into the School's Wi-fi system with a personal device in any other way than the official password enabled route
11. Deliberate Activities with any of the following characteristics or that by their nature would result in:
    - Wasting staff or other users' time or network resources, including time on remote systems and the time of staff involved in the support of those systems.
    - corrupting or destroying other users data.
    - violating the privacy of other users.
    - disrupting the work of other users.
    - using the Extranet/Internet in any way that denies services to other users (e.g. by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading or uploading large files).
    - continuing to use any item of software after being requested to cease its use because it is disrupting the correct function of the School's network or the Internet (for example, utilities designed to broadcast network-wide messages, etc.).
    - introduction of any malware (e.g. viruses, worms etc.)
    - e-mails spam/spoofing.
12. Damage to any computer hardware. The school reserves the right to charge for acts of willful vandalism. Use of the School's personal computers (including portables) to access the Internet through an unofficial or unauthorised route.
13. Printing of non-essential material and failure to check that the length of a document is reasonable before printing.
14. Unauthorised wireless access to the school Network.
15. Any other use deemed to be unacceptable by the designated person.

I understand if I break the rules in this Policy I will be punished in accordance with the School Discipline Policy, my parents will be informed and I may lose the opportunity to use the equipment.

Name			
Signature			
Form		Date	

Appendix 6

Queen Mary's Grammar School

Computer Network Student User Agreement

Name	

Queen Mary's Grammar School is pleased to offer access to the Internet and electronic Mail (e-mail) via the School's computer Network, subject to compliance with the School's Computer Network User Terms and Conditions and e-Safety Policy.

Access to email and the Internet will enable pupils to explore thousands of electronic educational resources while exchanging messages with Internet users throughout the world. Parents and guardians are warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While it is the school's intention to make Internet access available in order to further educational goals and objectives, pupils may find ways to access other materials as well. Our Internet Service Provider (ISP), School's Broadband, blocks access to unsuitable sites they are aware of. However, no guarantee can be given that access will be denied to all unsuitable sites. The school believes that the benefits to pupils of access to the Internet exceed any disadvantages. Ultimately, however, parents and guardians of pupils are responsible for setting and imparting the standards that their children should observe when using media and information sources. To this end, the School respects each family's right to decide whether or not to apply for access to the Internet, but it must be understood that pupils who do not have access will be unable to use the School's computer facilities at any time. Pupils who contravene the School's policy on the use of the Network and access to the Internet will be subject to the full range of disciplinary measures applied by the School and may be forbidden to use the Network.

The e-Safety policy and the Terms and Conditions are on the school website.

Pupils using the Internet should never divulge any personal information such as addresses and telephone numbers to other Internet users without first seeking guidance from a responsible adult.

It is important that all users report any breaches of the School's policies above to the e-Safety Adviser by themselves or others whether it be accidental or otherwise.

The e-Safety Officer is Mr. N. Canning, who may be contacted for further information.

Pupil Agreement

I have read and understood the School Computer Network User Terms and Conditions and the e-Safety Policy. I understand that if I contravene the e-Safety Policy, I will be punished and I may lose the opportunity to use the equipment. As a user of the School's network, I hereby agree to comply with the requirements of the Terms and Conditions and the e-Safety Policy and any other conditions that the School may from time to time, deem necessary.

Pupil Signature	Form	Date

Parental Permission

As the parent or legal guardian of the pupil signing above, I grant permission for my son/daughter to use the School's computer network and access networked computer services such as electronic mail and the Internet subject to the Terms and Conditions and Policies referred to. I understand that some material on the Internet may be objectionable, but I accept responsibility for my son/daughter complying with the school's rules when selecting, sharing and exploring information and media.

Parent/Legal Guardian Signature	Date

Appendix 7

Pupils' Online e-Safety Survey

E-Safety QMGS

1. What Year are you in?

- ○ 7
- ○ 8
- ○ 9
- ○ 10
- ○ 11
- ○ 12
- ○ 13

2. Do you feel safe using the Internet?

- ○ Yes
- ○ No

If no, what makes you feel unsafe?

3. Which of the following do you use to access the Internet?

- ☐ Games Console
- ☐ PC or MAC
- ☐ Laptop or Tablet
- ☐ Mobile Phone

4. Do your parents/carers discuss safe use of the Internet with you?

- ○ Yes
- ○ No

5. Do you use Social Networking sites, e.g. Facebook, Twitter, Ask.FM?

- ☐ Facebook
- ☐ Twitter
- ☐ Ask.FM
- ☐ MySpace
- ☐ Instagram
- ☐ Pinterest
- ☐ Bebo

Other (please specify):

6. Have you set your privacy settings on all your social networking accounts so that only friends can see what you post?

- Yes
- No
- N/A (I don't use Social Networking Sites)

7. Do you play online games?

- Yes
- No

8. What would your actions be if somebody says something hurtful to you online, or if something makes you feel uncomfortable?

9. Do you know what the following mean?

	Yes
Grooming	
Cyberbullying	
Sexting	
Trolling	
Identity Theft	
Phishing	
Flaming	

10. Have you experienced any of the following?

	Yes
Online bullying	
Sent/received a sex text	
Met someone online who has made you feel uncomfortable	
Been sent a message by an online troll	