E-Safety Policy

Statement

The Queen's School recognises that, in an increasingly digital world, the school needs to ensure that all staff and girls know how to conduct themselves safely and appropriately online.
The responsibility for E-safety is shared by all staff but is under the remit of the Designated Safeguarding Lead.

Aims
The purpose of this online safety policy is to:

- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Objectives
The objective of this policy is to safeguard all members of The Queen's School community online.

Related policies
This policy should be read in conjunction with the following policies;

- The safeguarding policy
- Whistleblowing policy
- Behaviour policy
- Anti-bullying policy includes reference to online bullying
- Child on child sexual abuse and harassment policy
- Confidentiality policy
- Staff Code of Conduct
- The Acceptable Use of IT agreements

The Queen's school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams

E-Safety Policy

E-Safety for staff
This should be read in conjunction with the Staff code of conduct, handbook and the Association of School and College Leaders (ASCL) guidance paper on social networking, social media and email regarding professional expectations of staff.

Staff must:

- Have an awareness and understanding of the provisions in place to filter and monitor IT activity and how manage them effectively and how to escalate concerns when identified.

- Provide effective supervision of devices both in the classroom, on educational visits, at fixtures, during ex-curricular activities and during pupil social times.

- Take steps to maintain awareness of how devices are being used by pupils.

- Report any safeguarding concerns to the DSL.

The school will:
• Provide the online safety policy to all members of staff for whom it is relevant to their job role, as part of induction.
• Provide up-to-date and appropriate E-Safety training for all staff for whom it is relevant to their job role, on a regular basis. This will cover the potential risks posed to pupils as well as our professional practice expectations.
• Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices. Misuse may lead to disciplinary action (see Disciplinary policy).
Ensure that staff who have contact with EYFS pupils are aware of the restrictions regarding their use of mobile phones (See EYFS Policy for the use of Cameras and Mobile Phone Devices)
• Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
• Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
• Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Procedures to use when responding to online safety concerns.

- If a member of staff has concerns about their own or a pupil's online activities, they must report concerns to the DSL. The DSL will follow the protocol established for safeguarding concerns (see Safeguarding Policy)

- If the concerns relate to another member of staff, they must report it to the Headmistress who will investigate the concerns (see also, Whistleblowing policy).
- Staff can also report concerns directly to CEOP (Child Exploitation and Online Protection)

See also Acceptable Use of IT agreement in appendix 1.

E-Safety for parents and carers

The Queen's School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. It is important to remember that pupils with a mobile phone often have unrestricted and unlimited access to the internet via 3G, 4G or 5G. Therefore, it is important that parents are aware of their children's online presence and activity in order to safeguard them from harm. Social media and private messaging can be a medium for bullying. It is important that parents are aware of how their children use social media and the dangers of children sharing and receiving inappropriate material, including pornographic images on social media or in private messages. Parents should encourage their children to report being sent inappropriate material or being pressured to send inappropriate material or online bullying. Reports can be made to;

- The parent
- The pastoral leadership team
- Directly to the platform
- To CEOP https://www.ceop.police.uk/Safety-Centre/

Harmful content can also be reported via https://reportharmfulcontent.com/report/
Parents and pupils can also utilise the report-remove tool to confidentially report sexual images of themselves online and remove them from the internet via
https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/
See also https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events.

E-Safety Policy

- Drawing their attention to the school online safety policy, resources and expectations in newsletters and on Firefly https://firefly.thequeensschool.co.uk/e-safety-guide
- Requesting that they read online safety information as part of joining our school
- Requiring them to read the school Acceptable Use agreement and discuss its implications with their children. See appendix 1a.

E-Safety for pupils
The Queen's School recognises the need to build the resilience of pupils to be able to engage appropriately and safely in the digital world.

This should be read in conjunction with the behaviour policy and anti-bulling policy. If a pupil is found to have breached the Appropriate Use guidelines, they will become subject to the interventions as set out in the Promoting Positive Behaviour policy.

Online challenges and hoaxes
https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes
A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. The DfE has produced guidance to help schools to deal with the increase of such incidents.

The school will assess the risk to children on a case by case basis and decide whether and/or how to address specific incidents, in line with the guidance.

Bullying and Child on Child sexual abuse and harassment
The school recognises that bullying can occur online through social media and private messaging. The school takes the view that any form of bullying in unacceptable and any pupil found to be engaging in online bullying will become subject to the Promoting Positive Behaviour policy. The school is aware that this may be happening to a pupil even if it is unreported. The school takes action through its anti-bullying policy to try to ensure that all online bullying is reported.

Child on child sexual abuse and harassment can also take place online. Pupils can receive unsolicited sexual images and videos ('nudes') or be pressured to send such material. The school is aware that this may be happening to a pupil even if it is unreported. The school takes action

through its Child-on-child abuse and harassment policy to try to ensure that all online sexual abuse or harassment is reported.

See also the Anti-bullying, Behaviour and Child on child sexual abuse and harassment policies.

Education

In the Senior School, E-safety is addressed through the curriculum, form time and awareness events;

Year 7

Form time: Go through the Acceptable Use policy. Look at common online activities and discuss the benefits and risks.

PSHE: Transition to senior school including friendships and appropriate use of technology/iPADs. Online gambling. (Sept)

Computing: E-Safety week and unit on the internet - workings, use and safety. (Jan/Feb)

Year 8

Form time

PSHE: Staying safe including e-safety. Sharing of sexual images, ie, 'nudes', 'sexting'..

Computing: E-Safety week and unit on Cyber security and cyber crime (Jan/Feb)

Year 9

Form time

PSHE: Free speech and the media

Computing: E-Safety week (Feb)

Year 10

Form time

PSHE: Your virtual World and online harassment

Computing: E-Safety week(Feb)

Year 11

Form time

PSHE: Sex and the media including pornography

Computing: E-Safety week(Feb)

Year 12

Form time

PSHE: E-Safety as you get older - your digital footprint.

Year 13

E-Safety Policy

Form time

We undertake an annual E-Safety survey to understand the digital world from the pupil's perspective. Results are shared with all staff so they can understand the potential risks. Pupils are regularly reminded that they should report any E-Safety concerns that they have to a teacher.
In the Lower School, E-safety is addressed through the curriculum, assemblies and awareness events.
Reception – Year 2
Computing: E-Safety Week (Feb), regular e-safety reminders within weekly lessons
Year 3-6
Computing: E-Safety Week (Feb)
E-Safety Unit taught to each year group in Autumn 1.
PSHE: Communication / technology units taught to each year group.

Acceptable use of IT
Clear guidance on the use of technology in the classroom and beyond for all users, including staff, pupils and visitors can be found in the following documents;

- For Staff – Information Security Policy, Data Protection Policy
- For Visitors - Visitors' Wi-Fi and School Computer Use

The Acceptable use of IT guidance can be found in appendix 1.

Parents are provided with an Acceptable Use of IT agreement to sign when their daughter joins the school.
Pupils, staff and parents are sent a link to the refreshed version of the agreement at the start of each new academic year.

Information on the management of personal data can be found:

- Information Security Policy, Data Protection Policy, Information and Records Retention Policy Internal
- School Privacy Notices and Information and Records Retention Policy

In order to create a community in which pupils can share concerns about online activity, we have created an anonymous online reporting tool in Teams that pupils can use to notify the DSL of any online activity that is of concern; https://forms.office.com/e/gPeJLjpUc3

E-Safety Policy

Roles and Responsibilities
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

Governing bodies - have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. They should review the effectiveness of your monitoring strategies and reporting process. Make sure that incidents are urgently picked up, acted on and outcomes are recorded. The safeguarding governor is responsible for ensuring standards are met. An annual review is conducted by the responsible governor, with members of the senior leadership team, the DSL and the Head of IT The results of the online safety review are recorded for reference and made available to those entitled to inspect that information. This forms part of the annual safeguarding governance framework.

Headmistress/SLT – supporting the DSL in ensuring standards are met. The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures

- act on reports and concerns

DSL - The DSL will work closely together with the Head of IT to ensure the standards are met. The DSL takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

Head of IT – The Head of IT has technical responsibility for;

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The Head of IT should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

External providers will:

- be members of the IWF(Internet Watch Foundation)
- have an up-to-date submission on the UK Safer internet Centre
- supply regular updates to filtering lists

All staff - have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

- provide effective supervision of devices
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL.

Staff should report concerns if;

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Filtering

The School utilises a web filtering server in order to monitor pupil and staff internet use. The server prevents access to inappropriate websites and logs all users' activity, whether they are using a School computer or their own mobile device. The server carries out automatic analysis of logs, in order to determine if a child or member of staff may be at risk owing to visiting, or attempting to visit, categories of websites including drugs, pornography, and intolerance. Following the analysis, a daily notification report is emailed by the server to the Head of Pastoral and the Deputy Head of Lower School, who judge whether intervention is required. Concerns regarding the activity of staff is passed to the Deputy Head or Headmistress.

Under the Acceptable use of IT agreement, pupils are not allowed to use any other internet connection from their mobile device when in School. Neither are they allowed to use 4G or 5G to access the internet or hotspot a connection for their phones or iPads.

No filtering system can be 100% effective. Risk assessments are conducted to understand the coverage of the filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in KCSiE and Prevent.

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves.

Monitoring

E-Safety Policy

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows the school to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

A variety of monitoring strategies are used to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users eg when pupils are using iPads in the classroom or in social times
- live supervision by staff on a console with device management software eg in the designated computer rooms
- network monitoring using log files of internet traffic and web access

Teachers may on request, ask IT staff to produce an activity log listing the websites that a pupil has visited over a particular period.

Incidents could be of a malicious, technical, or safeguarding nature. It should be clear to all staff how to deal with these incidents and who should lead on any actions.

There are situations where pupils may access the internet utilising their devices mobile data rather than the school's Wi-Fi. This is one reason why we educate pupils about internet safety. It is also important that parents take responsibility for monitoring their child's online activity on their mobile devices and share in the responsibility for educating them to be responsible online users. If we are concerned about a child's online activity, the DSL or Head of Year/Key Stage will contact the parents and work with them (and external agencies as appropriate) to support the child.

E-Safety Policy

Risk assessing

A review of filtering and monitoring is carried out annually to identify the current provision, any gaps, and the specific needs of your pupils and staff. This forms part of the safeguarding governance framework and includes;

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

To make your filtering and monitoring provision effective, the review will then inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

E-Safety Policy

The review should be done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

Checks will be made as part of the review to make sure that the system setup has not changed or been deactivated. The checks will include a range of;

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

We will record;

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

Ensuring that;

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

We will ensure that the filtering provider is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

The filtering system will be checked to ensure it is operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

The filtering system will be checked to ensure it;

- filters all internet feeds, including any backup connections
- is age and ability appropriate for the users, and be suitable for educational settings
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked
- provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

The filtering systems allows the DSL and Head of IT to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

E-Safety Policy

Appendix 1 Acceptable use of IT agreement for pupils
The following are not acceptable at The Queen's School and all pupils must abide by the following guidance.

As a pupil of The Queen's School, I will not

- send or display offensive, insensitive, provocative, or inappropriate messages
- take or send offensive, insensitive, provocative, or inappropriate photographs or videos
- use any audio or visual recording facility on my iPad in school without a teacher's permission
- use the internet to engage in activities that cause offence to staff or pupils, or are in contravention of the school's anti-bullying policy, or which are defamatory. This includes using the school's Virtual Learning Environment (Firefly - VLE), a social networking or other website from within or outside the school network.
- make videos or take images of myself or others using my iPad or mobile phone during the school day or when representing the school at a school function unless directed to do so by a teacher as part of a learning experience.
- share images of myself or other members of the school community on social media that may be damaging to the reputation of the school as I am an ambassador for the school. This includes images taken on school premises or at school functions including sports fixtures or images of pupils in school uniform (including sports kit).
- use the schools name or identifying features via hashtag, @ or other internet 'handle' without permission or guidance from a member of staff.
- use another person's username and password. Students should set strong passwords: a combination of at least 8 upper/lower case characters, numbers or punctuation marks.
- attempt to connect a personal laptop, mobile telephone, or other device to the internet using an unauthorised wireless connection, or a mobile data connection (e.g. a 3G/4G/5G connection) including an Apple "Personal Hotspot".
- attempt to use a virtual private network (VPN) connection from an iPad or from any other device.
- access undesirable materials from a school computer, personal laptop, mobile telephone or other device, which are racist, illegal, defamatory, pornographic, violent or potentially offensive to some people.
- share resources downloaded from the school's Firefly - VLE, or those from a website subscription, with anyone other than pupils and staff of the school.
- Violate copyright laws, including music and film downloads.

- Share a school password, wireless network key, or iPad passcode with another person
- Trespass in another person's network folder, work or files
- Intentionally waste limited resources (e.g. printing, network storage or network bandwidth)
- Employ the network/internet for commercial purposes
- Change the configuration or operation of equipment (e.g. backgrounds)
- Attempting to acquire unauthorised access to the school's network (hacking)
- Playing age-inappropriate computer games or accessing age-inappropriate web-sites
- Attempting to install software on any school computer
- Attempting to connect a personal laptop or other device to the school's network using a wired connection
- Knowingly trying to infect any school computer with a virus, by removable media (e.g. memory stick), via e-mail or by File Sharing
- Use my school e-mail address for purposes other than school work and activities
- Watch television programmes or videos for a disproportionate amount of time outside lessons

When using my iPad I will:

- Store my iPad in a locker when I cannot keep it with me at school.
- Notify IT staff if I lose my iPad as soon as is practicable.
- Keep my iPad passcode and my Apple ID secret.
- Not use my iPad on public transport when travelling between home and school.
- Only use my iPad in lessons when the teacher tells me to.
- Not use it outside my form room unless directed to do so by a teacher. Within my form room, I will be able to use my iPad to access learning resources, listen to music with earphones, use age-appropriate apps, and access the internet appropriately.
- Not take my iPad onto the gardens or sports' field unless specifically requested to do so by a member of staff.
- Not take my iPad into any changing rooms or toilets
- Use my iPad and not another pupil's.
- Upgrade the iPad OS operating system and school apps when instructed to do so by school IT staff, but not before.
- Not remove the mobile device management profile on my iPad or enrol any other device onto the school mobile device management system.
- Visit the IT Office if I have a new iPad to ensure it is connected to School IT systems.
- Bring to school with me each day: a fully-charged iPad, in a protective case, with a pair of earphones, Apple pencil.
- Copy school work to my OneDrive in order to: provide a backup, ensure sufficient free space on my iPad.
- Not change the date or time in the "Settings" app

The school is required to inform students if their IT use is monitored and for what purpose. The school currently uses electronic monitoring systems to monitor; logging on and off school computers, Microsoft Office365 use, Firefly - Virtual Learning Environment use, wireless network use, printer usage, attempts to penetrate network firewalls, attempts to connect personal devices to the school network, browsing the internet, use of students' personal work areas, connections to the school's mobile device management

system. In addition, physical monitoring of IT use takes place within the classroom and misuse can result in sanctions under the Promoting Positive Behaviour Policy.

This monitoring takes place in order to enforce this acceptable use policy, to help identify unauthorised use of students' accounts, to help prevent the spread of computer viruses and other threats, to formally record electronic communication between users and students via the Firefly - Virtual Learning Environment, to help prevent unauthorised access to the school network, to help conserve network resources, to help identify system faults, to install/uninstall apps on pupils' iPads, to help to meet the school's Safeguarding responsibilities, to assist in the planning and provision of IT equipment, and to help to recover pupils' work. The school reserves the right, in any case of suspected IT misuse, to use information recorded during monitoring as evidence. Further information about monitoring is available in the Senior School Pupil Privacy Notice available from https://www.thequeensschool.co.uk/privacynotices.