



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 DSL.

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
- Peer on peer sexual abuse and harassment policy
- Confidentiality policy
- Staff Code of Conduct
- The Acceptable Use policies

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 handbook and the ASCL guidance paper on Social networking, social media and email regarding professional expectations of staff.

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate E-Safety training for all staff 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.
- 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.

Taking action;

- If a member of staff has concerns about their own or a pupils online activities, they must report concerns to the DSL. The DSL will follow the protocol established for safeguarding concerns.
- If the concerns relate to another member of staff, they must report it to the Headmistress (see also, Whistleblowing policy).
- Staff can also report concerns directly to CEOP (see useful links).

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.

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

E-Safety Policy

- 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.
- 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 Policy and discuss its implications with their children.

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 girl is found to have breached the Appropriate Use guidelines, they will become subject to the interventions as set out in the Behaviour policy.

Bullying and Peer-on-Peer 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 is 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.

Peer-on-peer 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 Peer-on-peer sexual abuse and harassment policy to try to ensure that all online sexual abuse or harassment is reported.

See also the anti-bullying, behaviour and peer-on-peer 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)



E-Safety Policy

Year 8

Form time

PSHE: Staying safe including e-safety. 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

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.

Managing risks

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 Senior School Pupils - The Senior School IT Acceptable Use Agreement
- For Lower School Pupils - The Lower School IT Acceptable Use Agreement
- For Staff – Information Security Policy, Data Protection Policy



E-Safety Policy

- For Visitors - Visitors' Wi-Fi and School Computer Use

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. Pupils are not allowed to use any other internet connection from their mobile device when in School. Teachers may on request, ask IT staff to produce an activity log listing the websites that a pupil has visited over a particular time period. In addition, 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.

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

E-Safety useful links

<https://www.ceop.police.uk/safety-centre/>

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

<https://www.thinkuknow.co.uk/>

Further sources of information can be found in KCSIE September 2021, pages 150-152.



E-Safety Policy

Appendix 1 Remote Learning User agreement

The following guidance remains in place for those pupils who are accessing school virtually. This pupil user agreement applies in addition to the School's IT Acceptable Use policies and privacy notices.

Rules

- Use technology for school purposes only as directed by your teacher
- Ensure that an adult knows or is in the house when using technology
- Keep your passwords confidential and not reveal them to anyone
- Take responsibility for your behaviour and actions when using any remote learning platform, including the resources accessed and the language used
- Ensure all your communications with pupils, teachers or others using technology is appropriate
- Do not browse, download, upload or forward material that could be considered offensive or illegal and report any such material immediately to my teacher or my parent if you accidentally find any
- Do not record or take photos of classmates or teachers during a face-to-face meeting online
- Accept that the school can monitor and log your use of Firefly and make this information available to my teachers

Guidelines

Remember that any remote learning platform is an extension of the classroom and as such, you should conduct yourself accordingly

- Ensure you have the latest version of the Zoom app on your school iPad at all times
- When you receive a Zoom meeting link on a Firefly task from your teacher, you do not copy it anywhere else. This includes on social media or by using personal email
- Only access meetings and log in via the link sent by the teacher
- Zoom from an environment that is quiet, safe and free from distractions (your bedroom is not an appropriate room to work from)
- Be punctual for your interactive session and appropriately dressed for learning (that means no pyjamas)
 - Concentrate the best you can so you can remain focused during meetings
 - Exercise patience and respect with your teachers and fellow pupils
 - Offer feedback to teachers about your experiences and provide suggestions
 - Never record each other's online interactions
 - End the session as soon as the teacher indicates to do so and do not be late for other sessions.