Online Safety

Introduction

The School will safeguard and promote the welfare of girls in the School in accordance with Section 157 of the Education Act 2002 and in compliance with the statutory guidance Keeping Children Safe in Education (KCSIE) September 2023. This policy has been written in regard to Standard 8 (Safeguarding) and Standard 12 (Contact with parents/carers) of the National Minimum Standards (NMS) for Boarding Schools (September 2022).

Part F: Boarder's rights, advocacy, and complaints

NMS standard 12: Contact with parents/carers

12.1 Schools facilitate arrangements so boarders can contact their parents/carers and families in private, at a time that is suitable for both parties, considering relevant time zones for international students. Schools should operate proportionate systems to monitor and control the use of electronic communications in order to detect abuse, bullying or unsafe practice by boarders. Schools are sensitive and comply with individual children's circumstances such as restricted contact with families.

Part D: Safeguarding

NMS standard 8: Safeguarding

8.4 KCSIE sets out that boarding schools have additional factors to consider with regard to safeguarding. As such it will be important that the boarding school's child protection policy (and/or other policies if appropriate) reflect:

- the approach to harmful online content and how boarders' devices are managed in terms of bringing a device into the school, and harmful content that may already be downloaded on to it, and the opportunity to download harmful content via 3,4 and 5G that will bypass the school's filtering and monitoring systems.

In order to safeguard and protect children the school will have regard for the following guidance:

- Keeping Children Safe in Education (September 2023)
  - Keeping children safe in education 2023 - GOV.UK
  - KCSIE's Annex B contains additional information about specific forms of abuse and safeguarding issues, including, eg, children missing from education, cybercrime, mental health, preventing radicalisation, and sexual violence and sexual harassment between children in schools and colleges.
- Working Together to Safeguard Children (WT) 2018
  - Working Together to Safeguard Children - GOV.UK
- Prevent Strategy
  - Prevent duty guidance: England and Wales (2023) - GOV.UK

- Digital and technology standards in schools and colleges (March 2023)
    - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

The policy sets out measures for internet safety and includes a description of the school's use of filters and the school's monitoring of usage by students and staff.

1. Aims and Objectives

It is the duty of Queen Margaret's (QM) to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smartphones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and students), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection
- Prevent Strategy

- Safeguarding Code of Conduct;
- Girls Behaviour Policy
- Staff Behaviour Policy;
- Data Protection Policy and Privacy Notices;
- Safety and Supervision on School Trips Policy
- PSHE / RSE Policy; and
- IT Acceptable Use

At QM, we understand the responsibility to educate our students on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff, governors, and volunteers;
- "parents" includes students' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some students, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by students, in or out of school, will be dealt with under the school's [Behaviour Policy and / or Safeguarding and Child Protection Policy] as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the DSL, Deputy DSL, and Senior Leadership Team are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Head and the Senior Leadership Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at QM. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Head, IT Director and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the IT Director and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

3.4. IT Director

The DSL has delegated day to day responsibilities relating to online safety to the school's IT Director.

They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.

The IT Director will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

3.5. IT staff

The school's IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL.

3.6. Teaching and support staff

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Head and Senior Leadership Team as appropriate.

3.7. Students

Students are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

3.8. Parents and carers

QM believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

QM aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, students, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The DSL will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding and Online Safety Governor, the DSL and IT Director will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, harmful and illegal material. The school's filtering system is configured to allow access to different categories of websites for each year group of students and provides access to different categories in study and social browsing time periods.

If there is a good educational reason why a particular website, application, or form of content should not be blocked a student or member of staff can request for the website to be unblocked via an IT helpdesk ticket. If required this will be passed to the DSL for approval.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals to be identified. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the IT Department and the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone

accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the IT department and the DSL if they believe that appropriate teaching materials are being blocked.

Students:

Students must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the DSL or appropriate member of staff who will report to the DSL. Deliberate access to any inappropriate materials by a student will be dealt with under the school's Behaviour Policy. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, students can request for websites to be unblocked via an IT helpdesk ticket.

5. Education and training

5.1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When students use computers as part of their studies, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Students: the teaching of online safety

Online safety guidance will be given to students on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and Computer Science lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, students are taught about their online safety responsibilities and to look after their own online safety. Students can report concerns to the DSL and any member of staff at the school.

Students are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Students are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding and Child Protection / Anti Bullying / Behaviour Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The School annually asks parents to read and accept the IT Acceptable Use and Online Safety Policies. Parents and guardians are asked to check their child's device annually for harmful or concerning content.

6. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. [Devices issued to staff are encrypted, to protect data stored on them].

Staff are referred to the Staff Behaviour, safeguarding code of conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at QM are permitted to bring in personal devices for their own use.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any student nor to have any images, videos or other recording of any student on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies.

Students

Boarders must leave all personal devices in their respective Houses during the school day.

If students bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, and will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school allows students to use their own device for teaching and learning purposes. Students are required to adhere to the IT Acceptable Use when using their own devices for school work. The school recommends that students use a laptop. In particular, the IT Acceptable Use requires students to ensure that their use of their own devices for school work complies with this policy and the IT Acceptable Use.

Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by students will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the Deputy Head Pastoral to agree how the school can appropriately support such use. The Deputy Head Pastoral will then inform the student's teachers and other relevant members of staff about how the student will use the device at school.

7. Online Communications

Staff

Any digital communication between staff and students or parents / carers must be professional in tone and content. Under no circumstances may staff contact a student or parent / carer / recent alumni (i.e. students over the age of 18 who have left the school within the past 12 months) or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with students or parents / carers and recent alumni. Under no circumstances may staff contact a student or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system nor should students, parents and recent alumni / their parents / carers be added as social network 'friends' or similar.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Staff.

Students

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Students should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, students should contact the IT team for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to a member of staff who should then refer it to the IT DIrector/ DSL.

8. Use of social media

Staff

Although the school does not prohibit staff from using school devices for personal usage, staff must be aware that this will only be acceptable within reasonable levels. Staff must exercise caution when

using school devices for personal usage and be aware that all usage is filtered and can be monitored. Staff should not access social networking sites, personal email, any website or personal email which is unconnected with school work or business whilst in front of students.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Queen Margaret's School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
    - otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

Students

The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by students very seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

9. Data protection

Please refer to the Data Protection Policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and students are expected to save all data relating to their work to the school's central server / Google Drive Account as per the IT Acceptable Use Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or students should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT DIrector / IT Staff in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Director.

10. Password security

An effective system of passwords is a crucial tool to defend both the School and individuals. The School intends to follow the current guidance given to schools by the National Security Cyber Centre: Cyber security training for school staff - NCSC.GOV.UK

All staff have 2-Step verification turned on (it is optional for students). Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- Use a strong password
- Passwords must be at least 8 characters long
- Passwords under 13 characters in length must contain:
    - at least 1 lower case character (e.g. a, b, c)
    - at least 1 upper case character (e.g. A, B, C)
    - at least 1 numeric or special character (e.g. 1, 2, 3, !, @, %)
    - The password must not contain your username
    - The password must not contain your forename or surname
- not write passwords down; and
- not share passwords with other students or staff.

In addition to the above requirements, your password will be checked against a list of known bad passwords, that is managed by QM's IT department. Passwords can be checked to see if they are safe to use by visiting Pwned Passwords.

It is the responsibility of staff and students to ensure their password is safe and secure. If it is believed that a password may be compromised, steps must be taken to change it as soon as possible.

11. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites).

Please see, Taking, Storing and Using Images of Children Policy for more information.

12. Misuse

QM will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Safeguarding and Child Protection and Behaviour policies.

13. Complaints

As with all issues of safety at QM, if a member of staff, a student or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's IT DIrector and the DSL, in accordance with the school's Safeguarding and Child Protection Policy.

Claire Sheard
Senior Deputy Head
December 2023

Review Due: December 2024