



ONLINE SAFETY POLICY

Policy adopted by Community Committee on 13th March 2024, to be reviewed in 2025

Contents

1. Policy Aims	3
2. Policy Scope	3
2.1 Links with other policies and practices	4
3. Monitoring and Review	4
4. Roles and Responsibilities	4
4.1 The leadership and management team will:	4
4.2 The Designated Safeguarding Lead (DSL) will:	5
4.3 It is the responsibility of all members of staff to:	5
4.4 It is the responsibility of staff managing the technical environment to:	6
4.5 It is the responsibility of students (at a level that is appropriate to their individual age, ability and vulnerabilities) to:	6
4.6 It is the responsibility of parents and carers to:	6
5. Education and Engagement Approaches	7
5.1 Education and engagement with students	7
5.2 Vulnerable Students	7
5.3 Training and engagement with staff	8
5.4 Awareness and engagement with parents and carers	8
6 Reducing Online Risks	9
7 Safer Use of Technology	9
7.1 Classroom Use	9
7.2 Managing Internet Access	9
7.3 Filtering and Monitoring	10
7.3.1 Decision Making	10
7.3.2 Filtering	10
7.3.3 Dealing with Filtering breaches:	10
7.3.4 Monitoring	11
7.4 Managing Personal Data Online	11
7.5 Security and Management of Information Systems	11
7.6 Password policy	12

7.7 Managing the Safety of the School Website	12
7.8 Publishing Images and Videos Online	13
7.9 Managing Email	13
7.9.1 Staff	13
7.9.2 Students	13
7.10 Management of Learning Platforms	14
7.11 Management of ARBOR used to Record Children’s Progress	14
8 Social Media	15
8.1 Expectations	15
8.2 Staff Personal Use of Social Media	15
8.2.1 Reputation	15
8.2.2 Communicating with students and parents and carers	16
8.3 Students’ Personal Use of Social Media	16
8.4 Official Use of Social Media	17
9. Use of Personal Devices and Mobile Phones	18
9.1 Expectations	18
9.2 Staff Use of Personal Devices and Mobile Phones	18
9.3 Students’ Use of Personal Devices and Mobile Phones	19
9.4 Visitors’ Use of Personal Devices and Mobile Phones	20
9.5 Officially provided devices	20
10. Responding to Online Safety Incidents and Concerns	21
10.1 Concerns about Students’ Welfare	21
10.2 Staff Misuse	21
11. Procedures for Responding to Specific Online Incidents or Concerns	21
11.1 Youth Produced Sexual Imagery or “Sexting”	21
11.1.1 Dealing with ‘Sexting’	22
11.2 Online Child Sexual Abuse and Exploitation	23
11.2.1 Dealing with Online Child Sexual Abuse and Exploitation	23
11.3 Indecent Images of Children (IIOC)	24
11.4 Online bullying	24
11.5 Online Hate	25
11.6 Online Radicalisation and Extremism	25
12. Useful Links	26

Queen Elizabeth’s Grammar School

Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Queen Elizabeth's Grammar School, involving staff and students, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2023 and the Kent Safeguarding Children Board procedures. It will be revised at least annually.
- The purpose of Queen Elizabeth's Grammar School online safety policy is to:
 - Safeguard and protect all members of Queen Elizabeth's Grammar School community online
 - 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
- Queen Elizabeth's Grammar School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four 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

2. Policy Scope

- Queen Elizabeth's Grammar School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online
- Queen Elizabeth's Grammar School identifies that the internet and associated devices, such as chrome books, computers, tablets, mobile phones and games consoles, are an important part of everyday life
- Queen Elizabeth's Grammar School believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as students, parents and carers
- This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones

2.1 Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct
- School Behaviour Policy
- Child Protection Policy
- Curriculum areas, such as: Computing, Personal Social and Health Education (PSHE)
- Data Protection Policy
- Information Security Policy
- Electronic Information and Communications Policy

3. Monitoring and Review

- Queen Elizabeth's Grammar School will review this policy at least annually
 - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied - **see section 7 3 4**
- To ensure oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate
- All incidents of a safeguarding nature are logged and are reported to the Governing Body as part of the annual Safeguarding Report
- Any issues identified will be incorporated into the school's action planning

4. Roles and Responsibilities

- The school has appointed the Designated Safeguarding Lead, to be the Online Safety Lead
- Queen Elizabeth's Grammar School recognises that all members of the community have important roles and responsibilities to play with regards to online safety

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct and/or an AUP, which covers acceptable use of technology
- Ensure that suitable and appropriate filtering and monitoring systems are in place
- Work with technical staff to monitor the safety and security of school systems and networks
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all students to develop an age-appropriate understanding of online safety

- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- Audit and evaluate online safety practice on a continual basis, to identify strengths and areas for improvement

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training
- Work with staff to co-ordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Report online safety concerns, as appropriate, to the Leadership Team and Governing Body
- Work with the Leadership Team to review and update online safety policies on a regular basis (at least annually) with stakeholder input
- Meet regularly (at least twice a year) with the governor with a lead responsibility for safeguarding and online safety

4.3 It is the responsibility of all members of staff to:

- Contribute, if relevant, to the development of online safety policies
- Read and adhere to the online safety policy
- Take responsibility for the security of school systems and the data they use, or have access to
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- Embed online safety education in curriculum delivery, wherever possible
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally
- Take personal responsibility for professional development in this area

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Leadership Team
- Report any filtering breaches to the DSL and Leadership Team, as well as, the school's Internet Service Provider or other services, as appropriate
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures

4.5 It is the responsibility of students (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities
- Contribute, whenever possible, to the development of online safety policies
- Read and adhere to the school AUPs
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home
- Model safe and appropriate use of technology and social media
- Abide by the school's home-school agreement and AUPs Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Contribute to the development of the school online safety policies
- Use school systems, such as google classroom, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

5. Education and Engagement Approaches

5.1 Education and engagement with students

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst students by:
 - Ensuring education regarding safe and responsible use precedes internet access
 - Including online safety in PSHE, Computing, DLS and other programmes of study, covering use both at home and school
 - Reinforcing online safety messages whenever technology or the internet is in use
 - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
 - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

- The school will support students to read and understand the AUP in a way which suits their age and ability by:
 - Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
 - Rewarding positive use of technology by students
 - Implementing appropriate peer education approaches
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments
 - Seeking student voice when writing and developing school online safety policies and practices, including curriculum development and implementation
 - Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches

5.2 Vulnerable Students

- Queen Elizabeth's Grammar School is aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss
- Queen Elizabeth's Grammar School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students if necessary and appropriate
- Queen Elizabeth's Grammar School will seek input from specialist staff as appropriate, including the SENCO

5.3 Training and engagement with 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 online safety training for all staff on a regular basis, with at least annual updates. This will be achieved as part of existing safeguarding training and through specific online safety training – delivered by school leaders, the Kent Education Safeguarding Team and where appropriate, other professional organisations
- 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
- 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 students
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the school community

5.4 Awareness and engagement with parents and carers

- Queen Elizabeth's 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
- 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 such as parents' meetings, transition events and sports days
 - Drawing attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website
 - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement
 - Requiring them to read the school AUP and discuss its implications with their children

6 Reducing Online Risks

- Queen Elizabeth's Grammar School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace
We will:
 - Regularly review the methods used to identify, assess and minimise online risks
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches

7 Safer Use of Technology

7.1 Classroom Use

- Queen Elizabeth's uses a wide range of technology. This includes access to:
 - Computers, laptops, chromebooks and other digital devices
 - Internet which may include search engines and educational websites
 - School learning platform – Google Classroom
 - Email
 - Games consoles and other games based technologies
 - Digital cameras, webcams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community
- The school will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information
Supervision of students will be appropriate to their age and ability

7.2 Managing Internet Access

- The school will maintain an electronic record of users who are granted access to the school's devices and systems
- All staff, students and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Queen Elizabeth’s Governors and Leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit students’ exposure to online risks
- The Governors and Leaders are aware of the need to prevent “over blocking”, as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding
- The school’s decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school’s specific needs and circumstances
- Changes to the filtering and monitoring approach will be risk assessed by staff with the appropriate experience
- Significant changes to filtering and monitoring are directed by the Leadership Team following discussions with key staff; all changes to the filtering policy are logged and recorded
- Some changes to filtering occur as a result of standard procedural practice through our provider
- The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential

7.3.2 Filtering

- The school uses educational broadband connectivity through CoConnect
- The school uses
-
- wall web filtering which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature
- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list
- Student managed devices are restricted to school account during the school day to apply filtering and safeguarding policies
- Smoothwall Monitor is used for safeguarding on Staff and School accounts using school managed devices 24*7 (this will notify the Key Stage Support staff’ for lower alerts or DSLs directly if serious offences are detected)
- Any device connecting to the school network is subject to the schools filtering policy and logs
- 6th form devices on BYOD (Bring Your Own Device) are subject to the AUP, an electronically signed wireless agreement. These devices are filtered by Smoothwall when connected to the schools WIFI network
- Filtering may also apply outside of the school network using the school account on managed devices. This is provided on a best effort basis and normally at the request of a parent or guardian. This is not always technically possible
- The school works with both CoConnect and Smoothwall (web filter) to ensure that our filtering policy is continually reviewed

7.3.3 Dealing with Filtering breaches:

- The school has a clear procedure for reporting filtering breaches
 - If students discover unsuitable sites, they will be required to report this immediately to a member of staff. All students are taught to use the CEOP alert button when relevant. This always appears on their "home" page (bookmarked)
 - The member of staff will report the concern (including the URL of the site, if possible) to the Designated Safeguarding Lead and, or technical staff
 - The breach will be recorded and escalated as appropriate
 - Parents and carers will be informed of filtering breaches involving their child
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by: use of web filtering, monitoring through Smoothwall Monitor (DSL has access to this and receives email/call alerts above level 4)
- The school uses Smoothwall Monitor (safeguarding) for keyword detection and web activity logging. Smoothwall applies to the students' school account only, both in and outside of school. Designated staff (limited access) and DSL have access to this data and are emailed on triggers. Any critical trigger (such as danger to life) will immediately result in a phone call from Smoothwall.
- Classroom Management is provided by Classwise. Staff only have access to classroom management in school, during school hours with exception of the Network Manager and DSL(s) for urgent/critical intervention alerts.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. The DSL will be informed and will follow school safeguarding procedures appropriate to the nature and context of the concern
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998 and from May 25th 2018, by the EU General Data Protection Regulation
- Data Protection Policy (and EU General Data Protection Regulation, May 2018)

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly
 - Via appropriate secure remote access systems
 - Use of portable media is discouraged and strict guidelines will be provided regarding what may be stored
 - Portable media will be checked by an anti-virus /malware scan before use

- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly checking files held on the school's network
- The appropriate use of user logins and passwords to access the school network
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended
- Further information about technical environment safety and security can be found on AUPs for staff and students

7.6 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private
- From year 7 all students are provided with their own unique username and private passwords to access school systems; students are responsible for keeping their password private
- Student passwords must contain a minimum of 8 characters, including lower and upper case as well as special characters such as %, &, *

We require all users to:

- Use strong passwords for access into the school system
- Always keep their password private; users must not share it with others or leave it where others can find it
- Not to login as another user at any time

Additionally, staff are required to:

- Change their password regularly and as required by the school's IT systems
- Change the password immediately if any breach is suspected
- Password must not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)
- Passwords must not be the same or similar to previous passwords (the system will not allow for repeated use of the last 4 used passwords when setting new password)
- Staff passwords will be minimum 8 Characters long and changed annually at the start of each school year (you will be prompted to do this by the IT Department)
- Staff are forced to use 2 factor authentication on Google accounts for additional security protection. Devices that are used regularly provide an option to remember the specific device i.e. Chromebooks.
- In order to add a school account to a mobile phone, staff users will have basic mobile management enabled on their personal mobile devices that forces at least the following features: basic passcode enforcement (if the device has no pin, fingerprint, face ID or other security restriction the school account cannot be used on that device), hijacking protection, remote school account wipe, device reports (how many devices have synced with Google); these are simple features which help to protect the school account from loss/ransomware [Details here](#)

7.7 Managing the Safety of the School Website

- The school will ensure that information posted on its website meets the requirements as identified by the Department for Education (DfE)
- The school will ensure that its website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright
- Staff or students' personal information will not be published on the website; the contact details on the website will be the school address, email and telephone number
- The administrator account for the school website will be secured with an appropriately strong password
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community

7.8 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): Data security, AUPs, Codes of Conduct, social media and use of personal devices and mobile phones

7.9 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of Conduct
 - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email
 - School email addresses and other official contact details will not be used for setting up personal social media accounts
 - Teachers are discouraged from using personal devices for work emails – if used, passwords must be in place. Users must be aware that if the device is lost, the school will clear the device
- Members of the school community will immediately inform the DSL if they receive any offensive communication, and this will be recorded in the school safeguarding records
- Excessive social email use can interfere with the teaching and learning of students and will therefore be restricted so they may not access their phones between lessons and may only use phones within lessons with the permission of their teacher

7.9.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted
 - All members of staff are provided with a specific school email address to use for all official communication

- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents. Clear guidelines for reasonable staff email response times are available on the school website

7.9.2 Students

- Students will use school provided email accounts for educational purposes
- Students will sign an AUP (electronically) and will receive education regarding safe and appropriate email etiquette before access is permitted
- Whole-class or group email addresses may be used for communication outside of the school e.g. to share information about school trips

7.10 Management of Learning Platforms

- Queen Elizabeth's Grammar School uses Google Classroom as its official Learning Platform (LP)
- Leaders and staff will regularly monitor the usage of the Learning Platform in all areas, in particular, message and communication tools and publishing facilities
- Only current members of staff, students and parents will have access to the LP
- When staff and or students leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment
- Students and staff will be advised about acceptable conduct and use when using the LP
- All users will be mindful of copyright and will only upload appropriate content onto the LP
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive
 - If the user does not comply, the material will be removed by the site administrator
 - Access to the LP for the user may be suspended
 - The user will need to discuss the issues with a member of leadership before reinstatement. A student's parent or carer may be informed
 - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame
- A visitor may be invited onto the LP by a member of the Leadership; in this instance, there may be an agreed focus or a limited time slot

7.11 Management of ARBOR used to Record Children's Progress

- The school uses ARBOR to track students' progress and share appropriate information with parents and carers
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation

- In order to safeguard students' data:
 - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs
 - School issued devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft
 - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems
 - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

8 Social Media

8.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Queen Elizabeth's Grammar School community
- The term social media may include (but is not limited to): blogs; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of Queen Elizabeth's Grammar School community are expected to engage in social media in a positive, safe and responsible manner, at all times
 - All members of Queen Elizabeth's Grammar School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others
 - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities
- Concerns regarding the online conduct of any member of Queen Elizabeth's Grammar School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations Against Staff, Behaviour, Child Protection policies and Teacher Standards

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of Conduct and AUP

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing

appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school
- Members of staff should not identify themselves as employees of Queen Elizabeth's Grammar School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members. Accounts such as LinkedIn should be maintained with professionalism.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework
 - Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school

8.2.2 Communicating with students and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles
 - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead
 - If ongoing contact with students is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools
- Staff will not use personal social media accounts to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher
- Any communication from students and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead

8.3 Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age
- Any concerns regarding students' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and

behaviour. Concerns will also be raised with parents and carers as appropriate, particularly when concerning underage use of social media sites or tools

- Students will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and, or their location. Examples would include real or full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends and family, specific interests and clubs
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private and protected
 - Not to meet any online friends without a parent, carer or other responsible adult's permission and only when a trusted adult is present
 - To use safe passwords
 - To use social media sites which are appropriate for their age and abilities
 - How to block and report unwanted communications and report concerns both within school and externally

8.4 Official Use of Social Media

Queen Elizabeth's Grammar School's official social media channel is: Twitter – school account and Faculty Twitter accounts

- The official use of social media sites by the school only takes place with clear educational or community engagement objectives, with specific intended outcomes
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher
 - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only
 - Staff use school provided email addresses to register for and manage any official school social media channels
 - Official social media sites are suitably protected
 - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Safeguarding
 - All communication on official social media platforms will be clear, transparent and open to scrutiny
- Parents, carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community
 - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used
 - Any official social media activity involving students will be moderated by the school where possible
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels

Staff expectations

- Members of staff who follow and, or like the school social media channels will be advised to use dedicated professional accounts to avoid blurring professional boundaries
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Be professional at all times and aware that they are an ambassador for the school
 - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school
 - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared
 - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws
 - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so
 - Not engage with any direct or private messaging with current, or past, students, parents and carers
 - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from students

9. Use of Personal Devices and Mobile Phones

- Queen Elizabeth's recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within school

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, School Behaviour and Safeguarding
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times
 - All members of Queen Elizabeth's Grammar School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises
 - All members of Queen Elizabeth's community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour Policy
- All members of Queen Elizabeth's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or safeguarding policies

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Safeguarding, Data security and Acceptable Use
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time
 - Personal staff devices should be avoided where possible to reduce the risk of data loss. If personal devices are used to view data online you should avoid downloading data on the local device storage to safeguard that data. If data is downloaded/screenshotted this should be removed from the device and any other automated backups staff may have, i.e. student personal data from personal iCloud/Google accounts. Data stored in Google drive is available to be viewed online while a data connection is present i.e. a trip folder. Folders can be made available for offline use with the Google Drive app whilst keeping the data secure and encrypted and not stored on the devices file system.
 - Personal devices should have appropriate security (passcode, anti virus software etc.,) where applicable to help prevent the loss of data when accessing school resources.
 - If personal devices are enabled to access school data, care should be considered about who has access to that device i.e. young children and other family members who may see confidential information such as email etc.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times
 - Not use personal devices during teaching periods, unless permission has been given by a member of the Leadership Group, such as in emergency circumstances or for 2FA (two factor authentication) codes (CPOMS, Google, Arbor to name a few)
 - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations
- Members of staff are advised not to use their own personal phones or devices for contacting students or parents and carers
 - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of students and will only use work-provided equipment for this purpose
 - Directly with students, and will only use work-provided equipment during lessons/educational activities
- If a member of staff breaches the school policy, action will be taken in line with the School Behaviour and Allegations policies
 - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted

9.3 Students' Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences
- Queen Elizabeth's expects students' personal devices and mobile phones to be switched off during lessons. Personal devices must not be used between lessons or in the corridors
- If a student needs to contact his or her parents or carers they will be allowed to use a school phone
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff
 - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted
- Mobile phones and personal devices must not be taken into examinations
 - Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- If a student breaches the school policy, the phone or device will be confiscated and will be held in a secure place
 - School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Anti-Bullying Policy, Safeguarding Policy, or if it could contain youth produced sexual imagery (sexting)
 - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy and following government guidelines – www.gov.uk/government/publications/searching-screening-and-confiscation
 - Students' mobile phones or devices may be searched by a member of the Leadership Team, with the consent of the student or a parent or carer. Content may be deleted or requested to be deleted, if it contravenes school policies
 - Mobile phones and devices that have been confiscated will be released to parents or carers
 - If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Policy and other associated policies or procedures, such as: Anti-bullying, Behaviour, Child Protection and Image use
- The school will ensure appropriate signage and information is displayed to inform parents, carers and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy

9.5 Officially provided devices

- Members of staff will be issued with a work email address, where contact with students or parents or carers is required
- School devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff
- School devices will always be used in accordance with the Acceptable Use Policy and other relevant policies

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
 - Students, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure – this information will be distributed annually
- The school requires staff, parents, carers and students to work in partnership to resolve online safety issues
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Kent Education Safeguarding Team
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and, or the Education Safeguarding Team first, to ensure that potential investigations are not compromised

10.1 Concerns about Students' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns
 - The DSL will record these issues in line with the school's Safeguarding Policy
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy
- If necessary, allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)

- Appropriate action will be taken in accordance with the Behaviour Policy and Code of Conduct

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or “Sexting”

- Queen Elizabeth’s Grammar School recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ and KSCB guidance: “Responding to youth produced sexual imagery”
- Queen Elizabeth’s will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery

11.1.1 Dealing with ‘Sexting’

- If the school is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child Protection and Safeguarding policies and the relevant Kent Safeguarding Children Board’s procedures
 - Immediately notify the Designated Safeguarding Lead
 - Store the device securely
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image
 - Carry out a risk assessment which considers any vulnerability of student(s) involved; including carrying out relevant checks with other agencies
 - Inform parents and carers, if appropriate, about the incident and how it is being managed
 - Make a referral to Specialist Children’s Services and/or the Police, as appropriate
 - Provide the necessary safeguards and support for students, such as offering counselling or pastoral support
 - Implement appropriate sanctions in accordance with the school’s Behaviour Policy, but taking care not to further traumatise victims where possible
 - Consider the deletion of images in accordance with the UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance
 - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation
 - Review the handling of any incidents to ensure that best practice was implemented; the Leadership Team will also review and update any management procedures, where necessary

- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on or off school premises, using school or personal equipment
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so
 - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented
 - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request students to do so

11.2 Online Child Sexual Abuse and Exploitation

- The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns
- The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for students, staff and parents and carers
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally
- The school will ensure that the 'Click CEOP' report button is visible and available to students and other members of the school community – school homepage

11.2.1 Dealing with Online Child Sexual Abuse and Exploitation

- If the school is made aware of an incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's child protection and safeguarding Policies and the relevant Kent Safeguarding Children Board's procedures
 - Immediately notify the Designated Safeguarding Lead
 - Store any devices involved securely
 - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies)
 - Inform parents/carers about the incident and how it is being managed
 - Make a referral to Specialist Children's Services (if required or appropriate)
 - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on or off school premises, using school or personal equipment

- Where possible students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: <https://www.ceop.police.uk/safety-centre/>
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead
- If students at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised

11.3 Indecent Images of Children (IIOC)

- The school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC)
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team
- If made aware of IIOC, the school will:
 - Act in accordance with the school's Child Protection and Safeguarding Policy and the relevant Kent Safeguarding Children Board's procedures
 - Immediately notify the school Designated Safeguard Lead
 - Store any devices involved securely
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO
- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
 - Ensure that the Designated Safeguard Lead is informed
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via <https://www.iwf.org.uk>
 - Ensure that any copies that exist of the image, for example in emails, are deleted
 - Report concerns, as appropriate to parents and carers
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via <https://www.iwf.org.uk>
 - Ensure that any copies that exist of the image, for example in emails, are deleted
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate)

- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- Report concerns, as appropriate to parents and carers
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the Headteacher is informed
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy
 - Quarantine any devices until police advice has been sought

11.4 Online bullying

- Online bullying, along with all other forms of bullying, will not be tolerated at Queen Elizabeth's Grammar School
- Full details of how the school will respond to online bullying are set out in the Anti-Bullying Policy

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Queen Elizabeth's Grammar School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures
- The Police will be contacted if a criminal offence is suspected
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school
- If the school is concerned that a child or parent or carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child Protection Policy
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child Protection and Allegations policies

12. Useful Links

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Education Safeguarding Adviser (Online Protection): Ashley Assiter, (Monday/Tuesday/Wednesday) - 03000 423 164
- e-Safety Development Officer
 - esafetyofficer@kent.gov.uk Rebecca Avery - 03000 423 168
- Guidance for Educational Settings:

- [www kelsi org
uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)
- [www kelsi org
uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)
- [www kelsi org
uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links)
- Kent e-Safety Blog: [www kentesafety wordpress com](http://www.kentesafety.wordpress.com) and **register for an account to access the blog**

KSCB:

- <http://www.kscb.org.uk>

Kent Police:

- [www kent police uk](http://www.kent.police.uk) In an emergency (a life is in danger or a crime in progress) dial 999 For other non-urgent enquiries contact Kent Police via 101

Other:

- Smoothwall: www.smoothwall.com
- CoConnect: www.coconnect.co.uk

National Links and Resources

- Action Fraud: [www actionfraud police uk](http://www.actionfraud.police.uk)
- CEOP:
 - <https://www.thinkuknow.co.uk>
 - <https://www.ceop.police.uk/safety-centre/>
- Childnet: <http://www.childnet.com>
- Get Safe Online: <https://www.getsafeonline.org>
- Internet Matters: <https://www.internetmatters.org>
- Internet Watch Foundation (IWF); <https://www.iwf.org.uk>
- Lucy Faithfull Foundation: <https://www.lucyfaithfull.org.uk>
- NSPCC: <https://www.nspcc.org.uk/onlinesafety>
 - ChildLine: <http://www.childline.org.uk>
 - The Marie Collins Foundation: <https://www.mariecollinsfoundation.org.uk>
- UK Safer Internet Centre: <https://www.saferinternet.org.uk>
 - Professional Online Safety Helpline: <https://www.saferinternet.org.uk/professionals-online-safety-helpline>
- 360 Safe Self-Review tool for schools: <https://360safe.org.uk>

Signed _____ (Chair of Governors)

Date _____