E-SAFETY AND ACCEPTABLE USE OF IT POLICY

Queen's College, London

Due for review Summer 2027

Purpose of the Policy

At Queen's College London (QCL) we recognise the importance of promoting a safe and responsible digital environment for all members of our educational community. The purpose of this eSafety Policy is to establish clear guidelines and procedures that ensure the well-being, privacy, and security of our pupils, staff, and parents.

Aims

The policy aims to:

- Foster ethical and responsible use of technology.
- Protect users from online risks, including cyberbullying, inappropriate content, and online predators.
- Educate pupils about digital citizenship and their rights and responsibilities in the online world.
- Equip pupils with the necessary skills to navigate the digital landscape safely and responsibly.
- Establish mechanisms for incident reporting, intervention, and support.
- Continuously review and update the policy to address emerging eSafety concerns.

Scope

This policy applies to all members of the school community, including pupils, staff, governors, contractors and parents, and covers the use of school systems and personal devices both on and off site where this impacts the school, its pupils or its reputation.

Definitions

eSafety: the safe and responsible use of digital technologies, including the internet, social media and mobile devices.

Acceptable Use Policy (AUP): the set of rules governing how technology and digital systems may be used by members of the school community.

Cyberbullying: bullying behaviour conducted through digital technologies.

Principles

The School:

- recognises online safety as a safeguarding priority;
- promotes a preventative and educative approach;
- expects all users to act responsibly and respectfully;
- responds to concerns promptly and proportionately;
- works in partnership with parents and external agencies where appropriate.

Roles and Responsibilities

- **Designated Safeguarding Lead (DSL)** in conjunction with the IT department and HR department: is responsible for overseeing the implementation and adherence to this eSafety Policy. They will coordinate eSafety training and support, incident management, and liaison with external agencies as necessary.
- **Teachers, Staff and Governors:** All teachers and staff have a responsibility to ensure that eSafety principles are integrated into the curriculum, promote safe online practices, and report any concerns or incidents promptly.
- **Pupils:** Pupils must adhere to the Acceptable Use Policy (AUP) and follow the guidelines outlined in this policy. They should report any eSafety concerns to a teacher or the DSL.
- **Parents and Guardians:** Parents and guardians play a vital role in supporting their child's safe and responsible use of technology. They should familiarise themselves with the eSafety Policy, provide guidance to their child, and promptly report any concerns to the school.

Acceptable Use Policy (AUP) Summary

All users of Queen's College digital resources are required to comply with the Acceptable Use Policy (AUP). The AUP provides detailed guidelines on appropriate behaviour, responsible use of technology and consequences for violations.

Separate AUP documents apply to:

- pupils;
- staff; and
- parents.

These documents can be found in the appendices.

Digital Citizenship Education

Digital citizenship education is an integral part of our curriculum at Queen's College. It takes place across various subjects and year levels to ensure comprehensive coverage. The aim is to develop pupils' understanding of digital

rights, responsibilities, and the impact of their online behaviour on themselves and others. The following guidance is provided within the curriculum:

- Incorporate digital citizenship lessons within subjects such as Computer Science, PSHE, Future Frontiers and Thrive.
- Encourage critical thinking and responsible online behaviour through class discussions and activities.
- Promote respect, empathy, and ethical decision-making in online interactions.
- Provide age-appropriate guidance on cyberbullying, online privacy, and digital footprints.
- Engage pupils in projects and discussions that explore the positive use of technology for societal benefit.

Internet Filtering and Monitoring

To maintain a safe online environment, Queen's College employs internet filtering and monitoring systems. These systems are designed to block access to inappropriate content and websites that pose potential risks. They also allow for the monitoring of internet usage to identify any breaches of the AUP or potential eSafety concerns. Queen's College reserves the right to modify and update the filtering and monitoring systems as necessary to adapt to emerging threats.

Online Communication and Social Media

At Queen's College online communication and social media platforms must be used responsibly and in line with the AUP. Pupils are expected to communicate respectfully and considerately, ensuring that their online interactions contribute positively to the school community. The following guidance is provided for online communication and social media:

- Encourage pupils to use online communication platforms provided by the school for educational purposes.
- Teach pupils about online etiquette, privacy settings, and the potential consequences of sharing personal information.
- Promote responsible use of social media and discourage engaging in cyberbullying or harmful behaviour.
- Inform pupils about the school's guidelines for online communication and the consequences of violating them.

Data Protection and Privacy

Queen's College is committed to protecting the personal data and privacy of its pupils, staff, governors and parents. All personal information collected and processed by the school is done in accordance with relevant data protection laws and

regulations. The following guidance is provided for data protection and privacy:

- Ensure compliance with data protection laws and regulations, such as the General Data Protection Regulation (GDPR).
- Inform pupils, staff, and parents about the types of data collected, purposes of processing, and their rights regarding personal information.
- Implement appropriate security measures to protect personal data from unauthorized access, loss, or disclosure.
- Regularly review and update data protection practices to address emerging risks and requirements.

Online Safety Training and Support

- Staff: Queen's College provides regular eSafety training and professional development opportunities for staff to ensure they are equipped with the knowledge and skills to promote online safety effectively. Staff members are encouraged to report any eSafety concerns to the DSL promptly.
- Governors: All governors receive appropriate online safety training as part of their safeguarding and child protection training.
- Pupils: Pupils receive age-appropriate online safety education as part of their curriculum. Additionally, the College organises workshops, presentations, and awareness campaigns to reinforce eSafety principles. Pupils are encouraged to seek support from teachers or the DSL in case of eSafety concerns.
- Parents: The College offers online safety training sessions and resources for parents to support them in guiding their child's safe and responsible use of technology and also provides information and advice on various eSafety topics.

Incident Reporting

Any eSafety concerns, incidents, or breaches of the AUP should be reported immediately to a teacher or the DSL. The College has established clear reporting procedures to ensure swift action, support for those involved, and appropriate interventions. Incident reports will be treated confidentially and in line with relevant safeguarding and data protection policies.

Review

This eSafety School Policy is a live document. The document, along with the College's filtering and monitoring processes, will be reviewed annually by the Head of IT and Digital Learning; the DSL; the Bursar and it is submitted to Council for information. This will ensure its effectiveness and relevance. The DSL, in collaboration with the leadership team and relevant stakeholders, will assess emerging eSafety challenges, update policies and procedures, and communicate

any changes to the school community. Feedback from pupils, staff, and parents is encouraged to inform the ongoing improvement of the eSafety programme at the College.

Cyber-Bullying

This means bullying through the use of communication technology, such as mobile phone text messages, emails or websites. The most common forms are:

- Sending threatening or abusive text messages or emails, personally or anonymously.
- Making insulting comments about someone or posting fake or obscene photographs of another person on a website, social networking site or blog.
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email.

Pupils should ensure that their use of computers or mobile phones and other electronic devices does not render them liable to the accusation of cyber-bullying. Cyber-bullying can have a big impact on victims as a result of factors such as the invasion of personal space, the anonymity (at least initially) of the bully and the ability to broadcast upsetting messages and images rapidly to a potentially huge audience. A number of criminal offences can be committed during cyber-bullying, including harassment and using threatening, abusive or insulting behaviour.

Sanctions

Any breach of the code of conduct may lead to the automatic loss of access to all or part of the College network and/or the confiscation of a pupil's electronic device(s) e.g. mobile phone, tablet or laptop, while the matter is being investigated. Sanctions for breaches of this policy or for actions involving technology may be applied depending on the severity of the offence. For example, if a pupil brings their device uncharged to the lesson they will receive a negative daybook entry. Reflective time will be given to repeat offenders.

Pupils should be aware that the abuse of School and personal computer equipment, mobile phones and other electronic devices will be taken seriously. In cases where a pupil has been abusive and/or has committed an illegal offence the College's Behaviour, Management and Discipline policy and the Expulsion, Removal and Review policy will be adhered to. Misconduct during the holidays will be liable to College discipline if the welfare of other people or the reputation of the College are placed at risk.

Social Media

- Availability – use of social media sites are not permitted during the school day.
- Privacy levels - pupils must ensure any profile settings are set to private so that personal details and postings are only visible to nominated friends. This

applies to any and all social media including Facebook, Instagram, Snapchat and TikTok.

- Postings - pupils are reminded that they should only post material that would be deemed appropriate by a parent, teacher, university admissions department or by a potential employer. Postings should not contain any foul or abusive language or include uploads of words, images or film about:
    - The College which are derogatory and could damage our reputation.
    - Any teacher or support staff at QCL without their permission.
    - Any pupil at QCL which could be construed as abusive and offensive.
- Group sites:
    - Pupils are not allowed to set up sites about other people.
    - Pupils may not set up sites about any aspect of Queen's College or other schools or individuals which invite inappropriate comment.
    - A pupil setting up any other group is responsible for everything that is posted on that group. This includes the appropriateness of the title and nature of language in every posting. The administrator must, therefore, monitor it and delete it if inappropriate postings appear.
    - Must not be global and open for anybody to join - if a group is closed there will be some measure of control by Administrator(s).
- Gambling is against QCL rules. Pupils must not add gambling applications to their social media profile and should not enter any casino or gambling sites.

Online Learning

Pupils make use of computer technology as part of their everyday learning at QCL. However, in some situations pupils will be required to participate in online lessons which will ordinarily take place via Microsoft Teams. In such circumstances, all College rules continue to apply however, the following should be adhered to:

- Pupils should be ready to join each lesson at least five minutes prior to the published start time to ensure that the lesson can commence smoothly. They should open up Teams and wait patiently to join the meeting. Pupils should email their teacher if they have any difficulties accessing the lesson. Teachers will record absences as usual.
- The default setting is for all pupils to start online lessons with the microphone muted and the camera off (both front and back).
- No applications other than Teams should be open during a live lesson, unless instructed otherwise by the teacher. At the end of each lesson, every pupil should end the call.
- Where applicable, pupils should seek to find a suitable and appropriate location for the lesson where they are free from distractions and disturbance.
- All pupils should ensure that their behaviour and online etiquette are befitting and appropriate to the highest standards and expectations of QCL.
- Pupils should not record lessons or disseminate by any means pre-recorded lessons or other teaching resources. Any instances of disruptive behaviour will be followed up.

Appendix I: Technical requirements for 1-1 devices

Essential	Desirable
• Windows 10 or Windows 10 Pro operating system • Intel i5 or AMD Ryzen 5 processor • Minimum 8GB memory • Minimum 256GB SSD • 2 in 1 360 degree or 2 in 1 detachable keyboard • Stylus • Touch screen • Minimum 8 hours of battery life • Headphones • Camera installed • A protective case, clearly named	• Weight no more than 1.2 kg • 13″ screen • Full HD screen

Appendix II:
Pupils' Commitment to the ICT Acceptable Use Code of Conduct

This document is signed electronically by all pupils at the start of each academic year. It should be read in conjunction with the eSafety and Acceptable Use of IT Policy. By signing this document, pupils are also signing their agreement to all parts of the ICT AUP.

The College has a duty of care to ensure that each pupil at Queen's College uses computer equipment and the internet, as well as mobile phones and other communication devices, responsibly. Pupils should expect their computer use to be monitored, although this will be proportionate, i.e. only so far as is necessary and in such a way that potential intrusion on privacy is limited. The College network is available for use by the whole College community, including teachers and administrative staff. Pupils should, therefore, use computer equipment and the internet primarily for academic purposes and should not engage in any activity which may disrupt the effective operation of the network.

The code of conduct applies to use of any machines connected to the QCL network, as well as personal computers, laptops, mobile phones and other electronic devices.

- Pupils must never use another person's network account or allow their own network account to be used by another person; at all times pupils are responsible for the security of their own password. A pupil concerned that their password may be known to others should change it as soon as possible.
- Pupils must not attempt to access, send, display or store any offensive material (including images). This includes sending inappropriate messages or images via text (consensual and non-consensual self-generated intimate images and / or videos including those generated using AI, e.g. deep fakes).
- Pupils are forbidden from recording videos or images of any kind during lessons and activities unless given express permission by a teacher.
- Any form of electronic communication (including email, the internet or messaging systems) must comply with College and generally accepted standards of language and behaviour; abusive language is unacceptable.
- Pupils are forbidden from electronically sending over the internet or intranet or by any other means any confidential data, such as text or images, about the College or any personal data about individuals in it without permission.
- Pupils are not allowed to use internet filter by-pass methods or set up or use any wireless network independent of the School network (via 5G, VPN or by any other means) or use or operate any device such as a TV receiver.
- Pupils may connect private devices to the College's approved wireless network, while observing all the rules contained in this policy.
- Pupils are permitted to bring no more than one smart phone to College.

Sanctions

Any breach of the code of conduct will lead to the automatic loss of access to all or part of the College network and/or the confiscation of a pupil's electronic device(s) e.g. mobile phone, tablet or laptop, while the matter is being investigated. Sanctions for breaches of this policy or for actions involving technology may be applied depending on the severity of the offence, but pupils should be aware that the abuse of School and personal computer equipment, mobile phones and other electronic devices will be taken seriously. Misconduct during the holidays will be liable to School discipline if the welfare of other people or the reputation of the School are placed at risk.

Appendix III: Pupil Acceptable Use Policy (AUP)

This policy serves as a foundation for responsible and safe digital engagement within our educational community. As technology continues to shape the way we learn, communicate, and interact, it is crucial that we establish clear guidelines to ensure the well-being and integrity of our digital environment. The purpose of this AUP is to promote ethical and responsible use of technology, protect the privacy and security of all users, and empower our pupils as digital citizens. By adhering to this policy, we aim to create an inclusive and positive online space that encourages learning, collaboration, and creativity.

The following outlines the principles of the IT Acceptable Use Code of Conduct that is expected of all pupils in the College. Appendix B shows a summary of the pledge that pupils make to abide by this Code of Conduct via an online form at the start of each academic year.

Personal Computers/ Laptops

The use of Educational Technology (EdTech) in the classroom brings huge benefits to teaching and learning, but in order to facilitate these advantages, pupils are required to use their devices appropriately and come to lessons properly equipped

e.g. pupils must bring in their laptops fully charged each morning, along with their stylus and charging cable.

All pupils should bring their own laptop to the College to use for learning each day unless prior notice has been given by the College. Laptops are purchased by parents but must meet the minimum requirements set out in Appendix A of this policy.

It is essential that pupils abide by the rules and expectations set out in this policy, alongside the specific regulations relating to EdTech outlined below.

Rules regarding device set-up

- When on the College site, devices must only be connected to the College's wireless network and should not be tethered to any other network.
- Devices must be secured by a password.
- Devices must have the latest version of the following Office 365 Apps and have these configured to allow for automatic updates: Teams, Word, Excel, PowerPoint, OneDrive.
- The College OneDrive should be synced to each pupil's device so that offline work is possible
- Devices should have the latest operating system updates and security patches.

- Pupils must have the necessary software installed on their devices for Teaching and Learning, as instructed by staff.
- Anti-virus software must be installed and updated automatically.
- Pupils must ensure they carry their device around in a protective case.
- Pupil files must be saved to Office 365, OneDrive or shared areas to ensure that all data is backed up.
- Pupils are responsible for any loss of data that was not saved to the OneDrive.
- Devices should be charged every night at home and be ready to function for a full day at school each morning.

As stated above, mobile phones may not be used instead of laptop devices under any circumstances. If a pupil's laptop is broken and being repaired/replaced, parents may contact the pupil's Head of Section to see if a College laptop may be used in the interim.

As 1-1 devices are parent-owned, monitoring and filtering at home will be the responsibility of individual families. At school, the laptops will be monitored and filtered through the QCL Wi-Fi. Should a pupil be provided with a device owned by the College, the College will be responsible for the monitoring and filtering of these devices, including pupil use when they are off site.

The College's Network

The College's Computer Network, Intranet, Internet connections from the College network points and electronic communication platforms (such as email and Teams) are provided for pupils to use in association with academic work and associated activities.

The safeguarding of pupils remains paramount and the College reserves the right to prevent access to app stores and websites which it considers to be inappropriate for pupils. The College has systems in place to monitor pupils' use of the internet and to monitor communication across the network. This allows the College to maintain its duty of care in relation to safeguarding and to ensure pupils' compliance with the College's Rules.

A very effective security system is in place to prevent the introduction of computer viruses and to block access to websites which the College decides are undesirable. Systems also exist to audit and monitor individuals in their use of the College's computers and in their communication across the Internet.

The rules below serve a dual purpose:

- To prevent pupils from causing damage to software on their own computers and to the devices of others on the network;
- To prevent pupils from breaking the law by the misuse of computers.

- If any of these simple rules are broken, there is a very high probability that the perpetrator will be identified; every action on the network is logged and can be traced where there is reasonable cause to do so.

College Rules

- Access is a privilege, not a right; pupils must act responsibly to have continuing access to the College's network or permission to use their own personal equipment.
- Individual users are responsible for their behaviour and use of computer equipment, their communications over the network and for the security of their password. Pupils are not permitted to:
    - Wear a smart watch;
    - tamper with, cause damage to or steal computer property;
    - use another person's password or allow others to use their password;
    - access or attempt to access others' folders, work or files;
    - waste resources: this means occupying large amounts of storage space or network bandwidth and printing in volume, for anything other than academic purposes;
    - attempt to access sites containing 'adult' content e.g. sites where the 18+ age group is specified;
    - use chat programs on the College network other than those approved by the College;
    - install programs on the network or stand-alone machines or run them from any removable media or install any software or scripts on College equipment;
    - send email to all users ("spamming") unless the consent of a teacher has been obtained on each occasion;
    - play computer games, view or stream material that is not specified for academic purposes, unless the consent of a teacher has been obtained on each occasion;
    - set up a wireless network in QCL grounds or access a wireless network that is not provided by the School (via 5G or via any other means);
    - use a television receiver to access TV broadcasts;
    - use their device during a lesson in any way other than as the teacher has directed.
    - Download a VPN to circumnavigate the school filtering and monitoring systems
- The College reserves the right to examine equipment owned or operated in the College and removable media used with it, including network servers, network stations and stand-alone computers and mobile computing devices. Accessing or attempting to access, sending, displaying, editing, distributing, storing offensive material (including images or footage of behaviour judged by the College to be of a bullying type) on College or on portable media or devices of any kind, including mobile telephones, is not allowed.

- Pupils are permitted to bring one mobile phone to College. Pupils in The School and the Junior College must use their Yondr pouches. If a pupil forgets their Yondr pouch they must hand it into the front office. Pupils in the Senior College may keep their mobile phones with them about their person. They are not permitted to use their mobile phones during lessons unless the teacher has given them permission to do so and must only be used in the Senior Common Room and the Senior Library.
- Posting words, images or film about any institution or individual on the internet, without permission, infringes privacy, even if it was not intended to offend. Pupils can expect to be sanctioned if, either via the College
- network or outside it, they:
    - Record videos or images during lessons and activities unless given express permission by a teacher;
    - Upload words, images or film about the College, which are derogatory and could damage the reputation of the College;
    - Upload words, images or film about any teacher or support staff at the College without their permission;
    - Upload words, images or film about any pupil at the College, which could be construed as abusive and offensive;
    - Use foul or abusive language: all communication by email or over the internet must comply with College and generally accepted standards of language; email is expected to be used as a formal mode of communication with the courtesy of a subject line, salutation and signature.
- Pupils are not permitted to use any screen technology in the dining hall or any common area in the school such as the main corridor.
- Acceptable mobile use on College trips will be decided with the trip leader and a member of the SLT. This will be communicated to each pupil (and parents) prior to the start of the trip.
- Inappropriate use of smart watches or other electronic devices in lessons and in examinations will be subject to sanctions. The possession of a mobile phone or any other communication device in an examination room is an offence for which a pupil could be disqualified from the examination.
- The following are criminal offences and are, therefore, illegal:
    - Downloading, storing or sending files which are pornographic.
    - Downloading or sharing, either as donor or recipient, music, images or other material which is copyrighted.
    - Sending personal data about anyone other than oneself to a third party without the subject's permission (e.g. images or exam grades).
    - Any action which interferes with the operation of the College network, hardware, or cabling.
    - Any action which breaches, or attempts to breach, the security of the College network e.g. hacking, downloading potentially harmful files.
    - Creating an AI generated image of any pornographic nature
- Pupils are permitted to connect private devices to the College's approved

wireless network. However:

- When using the College's approved wireless network, pupils must observe all the rules contained in this policy;
- Pupils are permitted to bring no more than one smart phone to school;
- Pupils must use their Yondr pouch;
- Pupils must make every effort to maintain the security and integrity of their private devices, including installation of latest patches, updates and antivirus measures;
- The College reserves the right to inspect private devices for evidence of inappropriate behaviour or content;
- The College reserves the right to withdraw a pupil's wireless network access privileges at any time;
- The College's IT Department is not resourced to provide technical support, servicing or repairs for private devices.

Appendix IV: Parent Acceptable Use Policy (AUP)

What is an AUP?
We ask all pupils, staff and parents / carers in the Queen's College community to sign an AUP - a document that outlines how we expect them to behave when they are online and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media, both when on school site and outside.

Why do we need an AUP?
These rules were written to help keep everyone safe when using technology or online. QCL systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies - anything on a school device or using school networks may be viewed by a member of staff to keep pupils safe.

What am I agreeing to?
1. I understand that Queen's College uses technology as part of the daily life of the school when it is appropriate to support teaching and learning and the smooth running of the College, and to help prepare pupils for their future lives.
2. I understand that the College takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the College cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in QCL, and use of school-owned devices, networks and cloud platforms outside of school may be subject to filtering and monitoring. If I have bought a device for my daughter's use in school (meeting QCL specifications) I will ensure that certain software is installed, as advised by the IT Department. If I have bought a device through the College's preferred provider Easy4u, I understand that this software is already loaded on to the device.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative or threatening comments about others, including school staff, volunteers, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools so we expect certain behaviours from pupils when using it and wish for parents to support the College's guidance on social media.
6. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. QCL will only use images of my child publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online they will need positive input

from QCL and home so I will talk to my child about online safety on a regular basis.
8. I understand and support the commitments made by my child in the Pupil Acceptable Use Policy (AUP) which they will be required to sign. I understand that they will be subject to sanctions if they do not adhere to these rules.

Policy Information

Policy Title	E-Safety and acceptable use of IT Policy
Version	v. Approved
School	Queen's College London
Category	Safeguarding, Medical & Pupil Welfare
Statutory policy	No
Policy owner 1	DSL
Policy owner 2	
Approval	SLT
Submission to Council	Not required
Publish on website	Not required
Date of last review	Summer 2026
Approved by SLT	Approved
Staff notified	No
Review date	Summer 2027