QUEEN ETHELBURGA'S COLLEGIATE

E-SAFETY – DIGITAL WELLBEING POLICY

Review period: 01-31 May 2024 **Due for review:** May 2025	**This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:** The Education (Independent School Standards) Regulations 2014 Keeping children safe in education (DfE, 02 September 2024, updated 03 September 2024) (KCSiE) Working together to safeguard children (DfE, 26 March 2015, updated 23 February 2024) The National Minimum Standards for Boarding Schools (DfE, in force from 5 September 2022) Statutory framework for the Early Years Foundation Stage (DfE, 04 September 2023, updated 01 November 2024) Education Act 1996, 2011 Education and Inspections Act 2006 Equality Act 2010 Searching screening and confiscation Relationships and sex education Preventing bullying (DfE, 22 August 2013, updated 4 July 2017)	**To be viewed alongside the following related policies and documentation:** Anti-bullying Policy Acceptable Use Policies (AUPs) for staff and students Artificial Intelligence Policy Behaviour and Discipline Policy Child Protection and Safeguarding Policy Data Protection and Privacy Policy Esports Code of Conduct Risk Assessment (Welfare) Policy RSE Policy SEND Policy Staff Code of Conduct Visitor Policy	**Publication and availability for Staff, Parents, Carers and Prospective Parents:** This policy is published on the QE website and on the parent portal. It is available to staff on SharePoint.

	This policy has regard to the following guidance and advice: The Independent School Standards - Guidance for independent schools (April 2019) Equality Act 2010: advice for schools: departmental advice for school leaders, school staff, governing bodies and local authorities (DfE, May 2014) SEND code of practice: 0 to 25 years (DfE and DHSC, 11 June 2014, updated 12 September 2024) Teaching online safety in schools (DfE, 26 June 2019, 12 January 2023) Keeping children safe online | NSPCC Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated 11 March 2024). Anti-Phishing Working Group (APWG)) Meeting digital and technology standards in schools and colleges (DfE, 23 March 2022, updated 06 November 2024) Appropriate Filtering and Monitoring - UK Safer Internet Centre CEOP (Child Exploitation and Online Protection) Education (National Crime Agency) Childnet - Helping to make the internet a safe place My Safety Net ConnectSafely Safeguarding and remote education (DfE, 10 March 2021, updated 24 November 2022) Mobile phones in schools (DfE, 19 February 2024)		

QUEEN ETHELBURGA'S COLLEGIATE

E-SAFETY – DIGITAL WELLBEING POLICY

1. Introduction

1.1. This policy applies to Queen's Kindergarten and Chapter House Preparatory School, King's Magna Middle School, Queen Ethelburga's College, The Faculty of Queen Ethelburga's and Queen Ethelburga's Services (QES) - hereafter referred to as "**the Collegiate**". Staff from across the Collegiate are collectively known, and will be referred to, as "Team QE".

1.2. This policy also applies to Queen Ethelburga's holiday programmes, including Holidays@QE; QE Short Courses and International Summer School; and Camp QE.

1.3. The **E-safety – Digital Wellbeing Policy** applies to all members of the Collegiate community who have access to, store information on, and/or are users of, Collegiate ICT systems both in and out of school, including the use of personal electronic devices.

1.4. The policy applies to any use which affects the welfare of other members of the Collegiate community or where the culture or reputation of the Collegiate is put at risk. This includes any misuse of the internet or social media.

1.5. The staff and student **Acceptable Use Policies (AUPs)** are central to the **E-safety – Digital Wellbeing Policy** and should be consulted alongside this policy.

1.6. The **E-safety – Digital Wellbeing Policy** will be reviewed annually by the E-safety Committee, who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Student Council will be consulted regarding any changes to the **Student AUP**, and the staff body regarding any changes to the **Staff AUP**.

2. Aims

2.1. The Collegiate is committed to safeguarding the welfare of all students and recognises that an effective e-safety strategy is paramount in this.

2.2. Technology is a significant component in many safeguarding and wellbeing issues and e-safety can be categorised into four areas of risk:

2.2.1. **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

2.2.2. **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

2.2.3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes) and/or pornography, sharing other explicit images and online bullying. The UK Council for Internet Safety provide further guidance on responding to incidents and safeguarding children and young people: Sharing nudes and semi-nudes: advice for education settings working with children and young people (DSIT and UKCIS, 23 December 2020, updated 11 March 2024).

2.2.4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. Reports can be made to the Anti-Phishing Working Group if it is felt that students or staff are at risk.

2.3. The aim of this policy is to ensure a safe, beneficial and acceptable environment for all students and staff using the extensive ICT facilities provided by the Collegiate.

2.4. This policy in conjunction with the **Acceptable Use Policies (AUP) for staff and students**, aims to:

2.4.1. safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:

- exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials)
- the sharing of personal data, including images
- sexual violence and sexual harassment, including the sharing of unwanted explicit content and sharing nudes and semi-nude images and/or videos
- inappropriate online contact
- cyberbullying and other forms of abuse.

2.4.2. minimise the risk of harm to the assets and reputation of the Collegiate.

2.4.3. minimise excessive use of devices.

2.4.4. help all users take responsibility for their own ICT safety and wellbeing (i.e., limiting the risks that users are exposed to when using ICT).

2.4.5. ensure that students use ICT safely and securely and are aware of both external and peer to peer risks when using ICT.

2.4.6. protect personal data; and

2.4.7. prevent the unnecessary criminalisation of the user.

3. Responsibilities

3.1. The **Collegiate Board** will undertake an annual review of the Collegiate's safeguarding procedures (including reviewing filtering and monitoring) and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the Collegiate's curricular provision, ensuring relevance, breadth and progression.

3.2. The **Principal** is responsible for ensuring the safety (including online safety) of members of the Collegiate community, though the day-to-day responsibility will be delegated to members of the **E-safety Committee.**

3.3. The **E-safety Committee** consists of members of the Collegiate Board, QE Leadership Team, IT Team, Safeguarding and Welfare teams, including:

Chair of the Collegiate Board
Head of Student Welfare and Personal Development/DSL
Chair of the Committee/Head of Student Wellbeing
IT Representatives
Head of Chapter House
Designated Mental Health Lead/DDSL
Head of Personal Development/SMSC Link
Form Time and Assemblies Co-ordinator
Co-ordinator E-sports

3.4. The E-safety Chair organises regular meetings of the E-safety Committee.

3.5. The E-safety Committee takes day-to-day responsibility for e-safety issues in and out of school hours. The **E-safety Committee work with the Student Council** regarding any concerns or questions that arise. Meeting minutes are maintained to inform future e-safety.

3.6. The **Child Protection Team and E-safety Committee** are responsible for keeping up to date with e-safety issues in the use of internet and related technologies, and how these relate to children and young people.

3.7. The **Network Manager** is responsible for ensuring that the Collegiate's IT infrastructure is secure and that users may only access the Collegiate's networks through a username and password. Servers, wireless systems and cabling are securely located, and physical access is restricted.

3.8. The school **Local Area Network (LAN)** is protected by an active firewall.

3.9. In addition to this, there is a web filter (**Cisco**) that dictates the level of access given to the internet and is operated to ensure that students are unable to access any material that poses a safeguarding risk, including terrorist and extremist material.

3.10. **Filtering and monitoring**

3.10.1. Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material.

3.10.2. Management of the filtering and monitoring systems is reviewed annually and is the responsibility of the **Head of Student Welfare and Personal Development/DSL**, alongside the **Network Manager**, with the DSL taking lead responsibility for online safety and safeguarding and the Network Manager having technical responsibility.

3.10.3. The filtering system blocks access to harmful sites and inappropriate content.

3.10.4. Monitoring user activity on school and college devices is also an important part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Instead, monitoring allows user activity on school and college devices to be reviewed.

3.10.5. **Cisco** reports are sent daily to the Network Manager and Child Protection Team and acted on in line with the **Child Protection and Safeguarding Policy** and **Acceptable Use Policies**.

3.10.6. Https traffic will be decrypted and inspected as part of our filtering process using **Cisco** software.

3.11. There is restricted wireless access to the school LAN. The **Wide Area Network (WAN)** is managed off-site, and security is ensured through a separate VLAN, with virus protection updated daily.

3.12. The Collegiate **Microsoft (MS) Office 365** (MS 365) account enables users to access relevant file storage areas, as well as enabling users to report online issues electronically.

3.13. Students are not allowed to download executable files, and workstations are secured against user mistakes and deliberate actions.

3.14. The Network Manager **monitors** the use of the internet and email of all users, reporting any misuse to the E-safety Committee or Safeguarding Team as appropriate.

3.15. **Staff Responsibilities**

3.15.1. **All staff** are responsible for abiding by **the Staff Code of Conduct** and the **Staff AUP** and for implementing policies to safeguard and protect children.

3.15.2. Teaching and support staff must accept and comply with the **Staff AUP**, which is detailed in the Staff Handbook and can be accessed on SharePoint.

3.15.3. Staff must report any suspected misuse as detailed above.

3.15.4. New members of staff receive e-safety training as part of their induction programme, and all members of staff are kept up to date with e-safety issues though INSET and staff briefings.

3.15.5. Digital communications with students should be on a professional level and only through their **Collegiate MS 365 account**.

3.15.6. Teaching staff are responsible for monitoring ICT activity in lessons, and in extra-curricular and extended school activities. They should provide the necessary support for students and embed internet safety messages within lessons as appropriate.

3.15.7. Students are taught as part of their Spiritual, Moral, Social and Cultural Education and development (SMSC) to use ICT and the internet safely.

3.15.8. We aim to build resilience in students and develop their ability to protect themselves online and make the right choices. Students also receive support as part of a wellbeing programme.

3.15.9. Staff must be aware of e-safety issues related to the use of **mobile phones**, **cameras** and other **hand-held devices**.

3.15.10. Staff must ensure that such devices are used according to policy.

3.15.11. All members of staff are expected to maintain an appropriate level of professional conduct in their own internet use, including the use of social media, both within and outside school. **Any complaint about staff misuse must be referred to the Principal**.

3.16. **Staff Responsibilities and use of Collegiate Devices**

3.16.1. Collegiate devices will only be distributed once the member of staff has read and signed, the staff **Acceptable Use Policy**.

3.16.2. Devices can be checked at any time by relevant parties as designated by the Principal.

3.16.3. Staff should not use Collegiate electronic devices to conduct personal business/enterprise which would lead to personal gain.

3.16.4. Information such as media, photos, files and any other personal information must not be accessed or stored on the device.

3.16.5. Staff are welcome to use devices for personal use, in line with this and **Acceptable Use Policies**, but may not allow students to access staff members' personal devices at any time.

3.17. **Student Responsibilities**

3.17.1. **Students** are responsible for using the Collegiate ICT systems in accordance with the **Student AUP**, which parents must sign online before students are given access to Collegiate systems.

3.17.2. Students are taken through the **Student AUP** in form time and sign this in their student handbooks. The Student AUP is also discussed further in **Personal Development lessons** and **General Studies**.

3.17.3. Students must have a good understanding of research skills and the need to avoid plagiarism, as well as understanding the importance of reporting abuse, misuse or access to inappropriate materials.

3.17.4. The **Student AUP** makes it clear that failure to comply with its terms may lead to withdrawal of access, close monitoring of network activity, investigation into past network activity or, in more serious cases, criminal prosecution.

3.17.5. Careful consideration is also given to the use of **3G, 4G and 5G connection** on-site and the use of hotspots (further information is provided in the policy and the Acceptable Use Policies).

3.17.6. The Collegiate aims to educate students in the safe use of the internet and social media and continually offers guidance and support.

3.17.7. The Collegiate is aware that many students have unlimited and unrestricted access to the internet via mobile phone networks. Through this technology there are risks that students may sexually harass their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content whilst at school. If the Collegiate suspects that a student is accessing inappropriate material through their own 3G,4G or 5G network, then all devices are temporarily confiscated, and searches carried out in line with the Collegiate's **Behaviour and Discipline Policy** and **Child Protection and Safeguarding Policy**.

4. Teaching and Learning

4.1. Internet use is part of the curriculum and a necessary tool for learning. The internet is a part of everyday life for education, business and social interaction. Students use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

4.2. **E-safety** is **a focus in all areas of the curriculum**, and key e-safety messages are reinforced regularly, teaching users about the risks of internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour.

4.3. Staff should be vigilant in lessons where students use the internet and must ensure that devices are used in line with Collegiate policy.

4.4. Staff will be provided with sufficient e-safety training to protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues, including cyberbullying, sexual harassment, radicalisation cyber security and filtering and monitoring. The frequency, level and focus of such training will depend on individual roles and requirements.

4.5. The Collegiate's internet access is designed to enhance and extend education. Users will be taught what internet use is acceptable, and what is not, and given clear guidelines for internet use. The Collegiate will ensure that users are aware of copyright law regarding the copying and subsequent use of internet derived materials.

4.6. Staff should guide students to use online activities that will support the learning outcomes planned for the students' age and maturity. Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, for example, valid research about the Holocaust is likely to find information about Holocaust denial. The evaluation of on-line materials is a part of teaching/learning in every subject.

4.7. Where **generative Artificial Intelligence (AI)** and applications using AI are encouraged for teaching and learning purposes, staff will ensure students are aware of some of the dangers of this technology including information being out date and reflecting potential biases.

4.8. Students will also be instructed to ensure they do not use AI generated text or images as their own work but instead as the basis for developing their own learning and producing their own work. Students will also be warned to not enter sensitive personal data into AI websites.

4.9. Exam boards will each have their own policies relating to the use of generative AI and students must follow these when submitting work.

5. Internet use

5.1. The internet is a powerful tool which opens up new opportunities for students and staff. It can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

5.2. Students are given clear guidelines for what internet and email use is acceptable through the **Student AUP** and in lessons which use such technologies, as part of the curriculum in Personal Development (PSHCE), General Studies and ICT lessons, and in special presentations.

5.3. Key e-safety messages are also reinforced in assemblies and form time activities. Where appropriate, students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

5.4. **KCSIE (2024) Part 2** and DfE advice Teaching online safety in schools (DfE 26 June 2019, updated 12 January 2023) provide signposting to further advice, guidance and resources for schools, parents and children..

6. Management of website content

6.1. The Principal takes overall editorial responsibility and ensures that content is accurate and appropriate.

7. Storage of information and data

7.1. Under the **General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, staff and students must ensure that all data and information is stored using the Collegiate network. To protect personal data, the use of cloud-based storage and memory sticks/hard drives is no longer permitted.

8. QENET Wi-Fi and personal dongles

8.1. Students and staff may not use dongles purchased from mobile phone providers.

8.2. Mobile devices cannot be used as hotspots. QENET is the only authorised WIFI network. Mobile devices must not be used at inappropriate times or to access inappropriate material for the time of day, for example social networking sites or personal e-mail during prep.

8.3. Failure to follow these guidelines will lead to a minimum sanction of temporary confiscation of the device, although repeated breaches of this policy will lead to the student being prohibited from using any device which has been used inappropriately.

9. Mobile electronic devices (phones, laptops, tablets, smart watches and electronic trackers)

9.1. In line with the DfE guidance Mobile phones in schools (DfE, 19 February 2024), the use of mobile phones is prohibited throughout the teaching day (between 08:15 and 16:10), including during lessons, the time between lessons, breaktimes and lunchtime. This is to help students concentrate in class without distraction and to support positive behaviour in school.

9.2. Students from Year 6 upwards may keep possession of their mobile phones on the condition that they are kept in bags and not used, seen or heard. Students using their mobile phone during the school day will have it confiscated, in line with the **Behaviour and Discipline Policy**.

9.3. Students can contact their parents and families at break or lunchtime from a private space within the pastoral area. Students will have access to their laptops for educational purposes and communication via Microsoft Teams and email.

9.4. For Chapter House students, permission is required for them to bring a device which is capable of internet access or of storing text and images.

9.5. Whilst in school, Chapter House children must hand their device to their class teacher during registration, to be collected at the end of the day; it will be stored securely in the Head Teacher's office**. No mobile phones are to be used in the EYFS setting.** (See **Child Protection and Safeguarding Policy**).

9.6. Staff should not use their own mobile phone for personal reasons in front of students throughout the school day.

9.7. In boarding, mobile phones are permitted during free time, although their use is prohibited after lights out. Phones are collected in from younger students (up to Year 9) and this provision can be extended to students who persistently use their phones at inappropriate times. Further guidelines for mobile phones can be found in boarding policies.

9.8. **Mobile devices must not be used to directly take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission**. Students and staff are informed about the statutory framework regarding the sharing and publishing of photographs and videos, regardless of the media chosen. Staff must adhere to the **Child Protection and Safeguarding Policy** and **Staff Code of Conduct**.

9.9. Any use of mobile technology to intimidate, bully, harass, threaten or attempt to radicalise others or breach copyright laws will be counted as an infringement of network use and breach of discipline and will be dealt with in accordance with the **Collegiate's Behaviour and Discipline** and **Child Protection and Safeguarding policies**. This may result in disconnection from the network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, Collegiate and statutory guidelines are not breached.

9.10. Students are reminded that sending or posting images or videos of a sexual or indecent nature is **strictly prohibited** by the Collegiate and may constitute a criminal offence. The Collegiate will treat incidences of both sending and receiving prohibited images or text as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

9.11. **The Collegiate has the right to confiscate and/or search any mobile electronic device if it suspects that a student or staff member is in danger or has misused a device.** This will be done in accordance with the Collegiate's policy on **searching and confiscation**, as set out in the **Behaviour and Discipline Policy**.

10. Cyberbullying

10.1. Cyberbullying is the use of ICT, particularly mobile electronic devices, social networking sites, gaming and esports platforms,, deliberately to upset someone else.

10.2. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the **Collegiate's Anti-Bullying Policy**. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

10.3. Students should remember the following:

10.3.1. Always respect others - be careful what you say online and what images you send.

10.3.2. Treat others as you would like to be treated yourself.

10.3.3. Think before you send - whatever you send can be made public very quickly and could stay online forever.

10.3.4. Don't retaliate or reply online.

10.3.5. Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the Collegiate to investigate the matter.

10.3.6. Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.

10.3.7. Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

10.4. The Collegiate has clear procedures in place to support anyone affected by cyberbullying and if a student thinks that they are, or another person is, being bullied, they should talk to a member of staff or any trusted adult about it as soon as possible.

The following websites are useful resources for advice on internet use:
https://saferinternet.org.uk/
https://www.childnet.com/
https://mysafetynet.org.uk/
https://www.connectsafely.org/
CEOP Education (thinkuknow.co.uk)

10.5. The IT Team and staff will monitor the usage of shared areas of MS 365 and the intranet by students and staff regularly in all areas, in particular message and communication tools and publishing facilities. Students and staff will be advised on acceptable conduct and use when using the shared areas of MS 365 and intranet.

10.6. Only members of the current student body and staff community will have access to the shared areas of MS 365 and the intranet. When staff, students and other users leave the Collegiate their account or rights to specific school areas will be disabled.

10.7. Any concerns with content may be recorded and dealt with as follows:

10.7.1. Confiscation and searching the device in accordance with the procedures in the Collegiate's **Behaviour and Discipline Policy**.

10.7.2. The user will be asked to remove any material deemed to be inappropriate or offensive.

10.7.3. In some cases, the material may have to be removed by the site administrator, the Designated Safeguarding Lead or external agencies.

10.7.4. Viruses may be wiped from software on student and staff devices by the Head of IT.

10.7.5. Access to shared areas of MS 365 and the intranet for the user may be suspended.

10.7.6. The user will need to discuss the issues with a member of the Leadership Team before reinstatement.

10.7.7. A student's parent/carer may be informed.

10.7.8. Sanctions and support will be applied appropriate to the concern in line with the Collegiate's **Behaviour and Discipline Policy** and **Child Protection and Safeguarding Policy**.

10.7.9. Concerns about staff will be reported to the Principal following the referral process outlined in the **Child Protection and Safeguarding Policy** and **Whistleblowing Policy**. More information can also be found in the **Staff Code of Conduct** and **Staff Acceptable Use Policy**.

10.7.10. If there is a suggestion that a child is at risk of abuse or significant harm, including child-on-child abuse, the matter will be dealt with under the Collegiate's **Child Protection and Safeguarding** procedures.

10.7.11. The online abuse may be standalone or part of a wider pattern of child-on-child abuse (see the Collegiate's **Child Protection and Safeguarding Policy**).

11. Guidance for parents

11.1. The role of parents in ensuring that students understand how to stay safe online is crucial.

11.2. The Collegiate expects parents to promote e-safety and to:

11.2.1. support the Collegiate in the implementation of this policy and report any concerns in line with the Collegiate's policies and procedures.

11.2.2. talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour.

11.2.3. encourage their child to speak to someone if they are being bullied or need support.

11.2.4. have their home internet and digital devices set to age-appropriate settings and use appropriate internet filters to block malicious websites. These are usually offered free by your internet provider but require switching on.

11.3. Following the Coronavirus Pandemic, and the resulting greater reliance on online learning the Collegiate will signpost Guidance on safeguarding and remote education (DfE, 10 March 2021, updated 24 November 2022) for parents. This guidance offers online safety advice for parents and carers and a list of websites that promote safeguarding online.

11.4. The online resources mentioned previously provide useful information together with the DfE guidance Teaching online safety in schools (DfE, 26 June 2019, 12 January 2023)

11.5. Parents and carers should take note of any guidance on radicalisation given by **North Yorkshire Safeguarding Children Partnership (NYSCP)** .

11.6. The Collegiate only supports student access to age-appropriate social media platforms. Students who are below the minimum age will not be able to access the platform using the Collegiate WIFI network. Please note that the Collegiate can take no responsibility for any access to social media, or any other online material, which is made through private 3G, 4G or 5G connections.

11.7. If parents have any concerns or require any information about online safety, they should contact the **Head of Student Wellbeing**.

12. Visitors' access

12.1. Visitors are able to access the Collegiate's WIFI on request, with a visitor password and username. This provides limited access to the network and runs through '**Cisco**', the Collegiate's filter, to allow the Collegiate to monitor any inappropriate use.

13. Policy decisions

13.1. The Collegiate maintains a current record of all staff and students who are granted access to the Collegiate's electronic communications. All staff, parent/guardians and students must sign that they have read and understand the relevant AUP before using any Collegiate ICT resource.

13.2. The Collegiate will take all reasonable precautions to ensure that users access only appropriate material via filtering and monitoring systems. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Collegiate computer.

13.3. If students access inappropriate material from their personal devices the Collegiate takes no responsibility. This action can, however, be subject to investigation and sanction in line with Collegiate policy. Support can be provided, and students are encouraged to report any incident of misuse or concern to any member of staff they trust. The Collegiate also has an online virtual reporting system found in the QE Connect app, the '**Bully Box**', to which students can report bullying and attach any relevant information.

13.4. **Any user who accidentally comes across inappropriate or offensive material should do the following:**

13.4.1. Inform the Collegiate's Child Protection Team of the incident and give the website address. (This must be handwritten, not sent as an e-mail or forwarded).

13.4.2. Ask the Child Protection Team to log the web address, time and username.

13.4.3. The Child Protection Team will initiate an investigation. The categorisation of the material will be checked.

13.4.4. The outcome of the investigation will be relayed back to the E-safety Committee and logged.

13.4.5. Incidents will be reviewed by the E-safety Committee at each meeting.

13.5. **In the event of accidental access to illegal material:**

13.5.1. Inform the Collegiate's Child Protection Team of the incident and give the website address (this must be handwritten, not sent as an e-mail or forwarded).

13.5.2. **Do not show anyone** the content or make public the URL.

13.5.3. Make sure a reference is made of the incident.

13.5.4. The Child Protection Team may then go to the **Internet Watch Foundation (IWF)** website Eliminating Child Sexual Abuse Online | Internet Watch Foundation IWF and click the report

13.5.5. If reporting a URL, do not use copy and paste, type the URL.

13.6. **Any person suspecting another of deliberate misuse or abuse of technology should take the following action:**

13.6.1. Report in confidence to the Collegiate's Child Protection Team.

13.6.2. If the misuse is by a member of staff, this should be reported to the Principal.

13.6.3. The Child Protection Team should investigate the incident.

13.6.4. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of Collegiate rules, appropriate sanction will be enforced.

13.6.5. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, **Child Exploitation and Online Protection (CEOP) Command** or the police will be informed.

13.6.6. No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

14. Monitoring, risk assessment and development of policy

14.1. The school audits ICT use annually, to establish whether the **E–Safety – Digital Wellbeing Policy** is adequate and that the implementation of the E–Safety – Digital Wellbeing Policy is appropriate.

14.2. Methods to identify, assess and minimise risks will be reviewed every term and following any major incident.

14.3. Complaints of internet misuse, including the misuse of social media, will be dealt with under the relevant complaints procedure. Any complaint about staff misuse must be referred to the Principal.

14.4. All e–safety complaints and incidents will be recorded by the **Head of Student Wellbeing** or **Chair of the E-safety Committee**, including any actions taken.

14.5. Any issues (including sanctions) will be dealt with according to the Collegiate's **disciplinary and child protection and safeguarding procedures**. The DSL produces an **annual filtering and monitoring review** which is shared with the Collegiate Board and Queen Ethelburga's Leadership Team (QELT).

14.6. The E-safety Committee will consult the Student Council, to discuss issues, concerns or ideas the students may have.

14.7. The Collegiate will endeavour to draw from the whole Collegiate community, although this may require use of questionnaires rather than meetings with parents due to the distance most parents live from the Collegiate.

14.8. **Parents or guardians** indicate their support for the **E-safety – Digital Wellbeing Policy** by endorsing the Student AUP through the Parent Portal and by signing the **E-safety – Digital Wellbeing Policy** online. The Collegiate helps parents to understand e-safety issues through presentations and information made available on the website and via newsletters.

14.9. Risk assessment is in place, and regularly reviewed, with regards to CCTV, mobile devices and camera usage (refer to **the Child Protection and Safeguarding Policy** and **CCTV Policy**). Visitors and parents are asked not to post photographs of other people's children on social media sites without the express permission of those children's parents.

15. Virtual Private Networks

15.1. The use of VPN's is not permitted by staff or students, and this is reflected in the **Acceptable Use Policies**. Any use of a VPN is dealt with in line with the Collegiate intervention and sanctions systems.

16. Esports

16.1. The use of esports equipment and software at the school is allowed at the discretion of the **Esports Co-ordinator**, staff supervising esports and any other designated staff.

16.2. All use of esports is to be conducted in line with the **Esports Code of Conduct**.

17. Sharing of data and confidentiality

17.1. This policy has been reviewed in accordance with the **Data Protection Act (2018)** and the **UK General Data Protection Regulation (UK GDPR, 1 January 2021)**. More information about UK GDPR can be obtained from the Information Commissioner's Office (ICO) website.

17.2. The Collegiate accepts it has a duty of care to ensure individuals' data is kept safe and secure and the Collegiate privacy notices for staff, parents and students provide information regarding the personal information we collect and hold; what we do with it; who we can share it with; and how long we retain data. A privacy notice is available to view on the Collegiate website.

17.3. The Collegiate has a Data Protection Officer (DPO) who can be contacted directly at dpo@qe.org.

17.4. When sharing confidential information about a member of staff or student, the Collegiate has regard to its responsibilities under the **Data Protection Act (2018)** and to the **UK General Data Protection Regulation (UK GDPR, 1 January 2021)**, and where relevant, the **Education (Pupil Information) (England) Regulations (2005)**. Data Protection does not prevent the sharing of information for the purposes of keeping children safe.

18. Policy availability

18.1. Parents, prospective parents and carers can access this policy on the Parent Portal or the Collegiate website.

18.2. Hard or electronic copies of this policy can be requested from the PA to the Principal at esd@qe.org.

18.3. A hard copy can be made available to view during normal Collegiate opening hours, on request from the PA to the Principal at esd@qe.org.

18.4. This policy can be made available in large print if required.

18.5. Policies are available to all staff on the Home SharePoint page - Policies and Procedures 2023-25.

Version Control Table

Version Number	Purpose/Change	Author	Date
1.0	• The **annual** policy review concluded on 31 May 2024. • This policy was published with effect from **01 June 2024**.	• Head of Student Wellbeing	01.03.2024
1.1 Amendments and updates	• Updated links and references throughout this document and in the table on pages 1 and 2 to include: ➢ Keeping children safe in education (DfE, September 2024) (KCSiE) ➢ Keeping children safe online | NSPCC ➢ Mobile phones in schools (DfE, 19 February 2024)	• Head of Regulation	01.09.2024
1.2 Amendments and updates	• Updated links and references throughout this document and in the table on pages 1 and 2 to include: ➢ Statutory framework for the Early Years Foundation Stage (DfE, 04 September 2023, updated 01 November 2024) ➢ SEND code of practice: 0 to 25 years (DfE and DHSC, 11 June 2014, updated 12 September 2024) ➢ Equality Act 2010: advice for schools: departmental advice for school leaders, school staff, governing bodies and local authorities (DfE, May 2014) • **Section 9** on the use of mobile devices updated on 27.09.24 to reflect the latest Collegiate practice and guidance. • Added section **17 Sharing of data and confidentiality and 18. Policy availability**. • Appendix 1 **Filtering and Monitoring Review** removed.	• Head of Regulation • Head of Student Wellbeing	21.12.2024