



QUEEN ETHELBURGA'S COLLEGIATE E-SAFETY – DIGITAL WELLBEING POLICY

<p>Reviewed: 30 June 2023</p> <p>Due for review: June 2024</p>	<p>This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:</p> <p>The Education (Independent School Standards) Regulations 2014</p> <p>Keeping children safe in education 2023</p> <p>Statutory framework for the Early Years Foundation Stage (DfE, 31 March 2014, updated 12 July 2023) Applies from 4 September 2023</p> <p>National minimum standards for boarding schools, in force from 5 September 2022</p> <p>Working Together to Safeguard Children 2018 (updated 1 July 2022)</p> <p>Preventing bullying (DfE, 22 August 2013, updated 4 July 2017)</p> <p>Education Act 1996, 2011</p> <p>Education and Inspections Act 2006</p> <p>Equality Act 2010</p> <p>Searching screening and confiscation</p> <p>Relationships and sex education</p> <p>This policy has regard to the following guidance and advice:</p> <p>Teaching online safety in schools (DfE, 26 June 2019, 12 January 2023)</p>	<p>To be viewed alongside the following related policies and documentation:</p> <p>Anti-bullying Policy</p> <p>Acceptable Use Policies (AUPs) for staff and students</p> <p>Artificial Intelligence Policy</p> <p>Behaviour and Discipline Policy</p> <p>Child Protection and Safeguarding Policy</p> <p>Data Protection and Privacy Policy</p> <p>Risk Assessment (Welfare) Policy</p> <p>RSE Policy</p> <p>SEND Policy</p> <p>Staff Code of Conduct</p> <p>Visitor Policy</p>	<p>Publication and availability for Staff, Parents, Carers and Prospective Parents:</p> <p>This policy is published on the QE website and is available to staff on SharePoint.</p>
--	---	--	---



	<p>Safeguarding and remote education guidance</p> <p>How to Keep Children Safe Online When Using Social Media</p> <p>Advice for Parents and Carers on Cyberbullying.</p> <p>Sharing nudes and semi-nudes: advice for education settings working with children and young people.</p> <p>Anti-Phishing Working Group (APWG)</p> <p>Meeting digital and technology standards in schools and colleges</p> <p>Appropriate Filtering and Monitoring - UK Safer Internet Centre CEOP Education (thinkuknow.co.uk)</p> <p>www.childnet.com/</p> <p>mysafetynet.org.uk/</p> <p>connectsafely.org/</p> <p>CEOP Education (thinkuknow.co.uk)</p> <p>Advice for Parents and Carers on Cyberbullying</p> <p>Safeguarding and remote education (DfE, 10 March 2021, updated 24 November 2022)</p> <p>Safeguarding Essentials – How To Keep Children Safe Online When Using Social Media</p>	
--	---	--

Introduction

This policy statement 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". This policy also applies to Queen Ethelburga's holiday programmes, including Holidays@QE; QE Summer Schools; and Camp QE.

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. 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.

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

Aims

The Collegiate is committed to safeguarding the welfare of all students and recognises that an effective e-safety strategy is paramount in this. Technology is a significant component in many safeguarding and wellbeing issues and e-safety can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **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.
- **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 - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people).
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. Reports can be made to the Anti-Phishing Working Group (<https://apwg.org/>) if it is felt that students or staff are at risk.

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 and, together with the AUPs, to:

- 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.
- to minimise the risk of harm to the assets and reputation of the Collegiate
- to minimise excessive use of devices
- to 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)
- to ensure that students use ICT safely and securely and are aware of both external and peer to peer risks when using ICT
- to protect personal data; and
- to prevent the unnecessary criminalisation of the user.

Responsibilities

The **Collegiate Board** is responsible for the approval of the **E-safety – Digital Wellbeing Policy** and reviewing its effectiveness. 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.

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** which consists of:

Chair of the Collegiate Board

Head of Student Welfare and Personal Development/DSL

Chair/Head of Student Wellbeing

IT Representatives

Head of Chapter House

Head of Boarding

Pastoral Lead – Student Wellbeing

Head of Personal Development/SMSC Link

Chapter House Representative

EDI officer

The E-safety Chair organises regular meetings of the E-safety Committee. The E-safety Committee takes day-to-day responsibility for e-safety issues in and out of school hours. The team consists of members of the Collegiate Board, QE Leadership Team, IT Team, Safeguarding and Welfare teams. The minutes from the E-safety Committee's meetings are sent to the Student Council meetings for their input and support. Meeting minutes are maintained to inform future e-safety.



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.

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. The school Local Area Network (LAN) is protected by an active firewall. In addition to this, there is a web filter (Smoothwall) 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.

Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material. 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. The filtering system blocks access to harmful sites and inappropriate content. 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. Smoothwall reports are sent daily to the Network Manager and Child Protection Team and acted on in line with the Child Protection and Safeguarding and Acceptable Use Policies. Https traffic will be decrypted and inspected as part of our filtering process using Smoothwall software.

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. The Collegiate 365 account enables users to access relevant file storage areas, as well as enabling users to report online issues electronically. Students are not allowed to download executable files, and workstations are secured against user mistakes and deliberate actions. The Network Manager monitors the use of the internet and email of all users, reporting any misuse to the E-safety Committee.

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.

Teaching and support staff must accept and comply with the Staff AUP, which is detailed in the Staff Handbook, and must report any suspected misuse as detailed above. 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 through INSET and staff briefings. Digital communications with students should be on a professional level and only through their Collegiate Microsoft Office 365 account. 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. Students are taught as part of SMSC to use ICT and the internet safely, and 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 wellbeing programme. Staff must be aware of e-safety issues related to the use of mobile phones, cameras and other hand-held devices, and ensure they are used according to policy. 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.

Collegiate devices will only be distributed once the member of staff has read and signed, the staff Acceptable Use Policy. Devices can be checked at any time by the E-safety Committee and supporting safeguarding staff. Staff should not use Collegiate electronic devices to conduct personal business/enterprise which would lead to personal gain. Information such as media, photos, files and any other personal information must not be accessed or stored on the device. 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.

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. Students are taken through the 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. 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. The 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.

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

Teaching and Learning

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. 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.

Staff should be vigilant in lessons where students use the internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with Collegiate policy. 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.

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.

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.

Where generative 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. 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.

Internet use

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. Students are given clear guidelines for what internet and email use is acceptable through the 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. 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. KCSIE (2023) Part 2 and DfE Advice for Schools 'Teaching Online Safety in Schools (June 2019)' provide signposting to further advice, guidance and resources for schools, parents and children and



a selection of these resources are promoted through the Pastoral Care section of the Collegiate's website.

Management of website content

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

Storage of information and data

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.

QENET Wi-Fi and personal dongles

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

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.

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.

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

Mobile electronic devices for students in Year 6 and above are permitted both in boarding houses and in academic school. During the school day, phones are only to be used by students outside of lessons, unless permission had been given by the lesson teacher. Headphones must not be used while moving around the grounds.

Chapter House students are only allowed to have mobile electronic devices in school with advance permission from parents. All devices will be kept in a secure place by the form teacher during the day and handed back to the students at the end of the day. No mobile phones are to be used in the EYFS setting. (See **Child Protection and Safeguarding Policy**).

In lessons, mobile devices should be turned off and kept in a bag or pocket (i.e., not visible, and silent) unless permission has been given by the classroom teacher. In the event of a mobile device being used in a lesson without permission from the teacher, the device should be confiscated and given to the pastoral team.

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.



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.

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.

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.

The Collegiate has the right to confiscate and 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.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile electronic devices and the internet, deliberately to upset someone else. 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.

Students should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- 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.

- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

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 \(thinkuknow.co.uk\)](https://www.thinkuknow.co.uk/)

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

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

- Confiscation and searching the device in accordance with the procedures in the Collegiate's Behaviour and Discipline Policy.
- The user will be asked to remove any material deemed to be inappropriate or offensive.
- In some cases, the material may have to be removed by the site administrator, the Designated Safeguarding Lead or external agencies.
- Viruses may be wiped from software on student and staff devices by the Head of IT.
- Access to shared areas of Office 365 and the intranet for the user may be suspended.
- The user will need to discuss the issues with a member of the Leadership Team before reinstatement.
- A student's parent/carer may be informed.
- 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.



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

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

Guidance for parents

The role of parents in ensuring that students understand how to stay safe online is crucial. The Collegiate expects parents to promote e-safety and to:

- support the Collegiate in the implementation of this policy and report any concerns in line with the Collegiate's policies and procedures.
- 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.
- encourage their child to speak to someone if they are being bullied or need support.
- 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.

Following the Coronavirus Pandemic, and the resulting greater reliance on online learning the Collegiate will signpost <https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19> for parents. This site has a list of websites we recommend parents use to promote safeguarding online.

The online resources mentioned previously provide useful information together with the DfE guidance [Advice for Parents and Carers on Cyberbullying](#). Parents and Guardians should take note of any guidance on radicalisation given by North Yorkshire Safeguarding Children Board.

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. Below is an article which gives more information about different applications and their minimum age for use. 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.

[How To Keep Children Safe Online When Using Social Media](#)

The Collegiate also has a Pastoral Care section within its website which offers advice and support on current issues and challenges students may face. This can be found at <https://www.qe.org/home/pastoral-care>



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

Visitors' Access

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 'Smoothwall', the Collegiate's filter, to allow the Collegiate to monitor any inappropriate use.

Policy Decisions

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.

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.

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 also 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 to which students can report bullying and attach any relevant information.

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

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).
2. Ask the Child Protection Team to log the web address, time and username.
3. The Child Protection Team will initiate an investigation. The categorisation of the material will be checked.
4. The outcome of the investigation will be relayed back to the E-safety Committee and logged.
5. Incidents will be reviewed by the E-safety Committee at each meeting.

In the event of accidental access to illegal material:

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)
2. Do not show anyone the content or make public the URL



3. Make sure a reference is made of the incident
4. The Child Protection Team may then go to the Internet Watch Foundation (IWF) website at www.iwf.org.uk and click the report
5. If reporting a URL, do not use copy and paste, type the URL. In the event of unsolicited illegal material received by e-mail, the Child Protection Team should report to Easynet on abuse@uk.easynet.net or contact the Easynet helpdesk on: 0845 333 4568.

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

1. Report in confidence to the Collegiate's Child Protection Team.
2. If the misuse is by a member of staff, this should be reported to the Principal.
3. The Child Protection Team should investigate the incident.
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.
5. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
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.

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

The E-safety Committee will consult the Student Council, to discuss issues and any concerns or ideas the students may have. The Collegiate will endeavour to draw from the whole Collegiate community, although this may require questionnaires rather than meetings with parents due to the distance most parents live from the Collegiate.



Virtual Private Networks

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.

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.

Risk assessment is in place, and regularly reviewed, with regards to CCTV, mobile devices and camera usage (See 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.

Personal data is managed in line with the **Collegiate's Data Protection and Privacy Policy**, which gives further details about the management, storage and release of personal data in line with the Data Protection Act.



Appendix 1

Filtering and Monitoring Review

The Filtering and Monitoring Review is to be added to Appendix 1 following the Collegiate board meeting on Friday 15th September 2023.