KING'S COLLEGE INTERNATIONAL SCHOOL
BANGKOK

Reference number		Policy name	Digital Responsibility (E-Safety) & Acceptable ICT use Policy

Person(s) responsible	Jerome Marshall (Primary DDSL) Matthew Gibson (Senior DDSL)	Date of next review	January 2025

Vision, mission and values	**Mission** To produce well-rounded, academically successful, happy young men and women. **Vision** To engage, inspire and extend our students, our staff and the wider community. **Values** To create a community where everyone mirrors our values of good manners, kindness and wisdom.
Purpose	The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich their learning.

Approved by	SLT	Date	29/10/2023

Introduction

Digital responsibility is a priority at King's College International School Bangkok. While we actively embrace all of the benefits of the Internet, we are equally vigorous in embedding safe working practices amongst the whole school community. We are committed to ensuring that we balance the life-giving and creative elements of this learning with an approach which brings best practice in enabling responsible behaviour for learning and well-being.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2023, RSE guidance 2021 and other statutory and non-statutory documents. The school's Digital Responsibility policy operates in conjunction with other policies including those for: Anti-Bullying, Teaching and Learning, Data Protection, Safeguarding and Child Protection; Staff Code of Conduct, Acceptable Use Policy (AUP) and Student Acceptable Use

Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Our School Context:

- EYFS:
    - EYFS students use the interactive whiteboard in class (Nursery and Reception only) during independent learning time. They also have occasional access to iPads.
- Primary:
    - KS1students have shared iPads (1:2) that are stored between two classrooms.
    - KS2 students have 1:1 iPads that are stored in their own classroom.
    - A class set of laptops is used for teaching Computer Science.
- Senior:
    - Senior students bring their own device to school. This should be a laptop preferably although tablets are accepted.

The 3 key categories of risk

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as making or sharing sexually explicit material, cyberbullying or downloading or viewing illegal content.

We keep children and young people safe by:

- providing clear and specific directions to staff and volunteers on how to behave online through our code of conduct
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate

- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Digital Responsibility in the curriculum

Early Years

In Early Years, digital responsibility is taught in relation to Personal, Social and Emotional Development (PSED) and Understanding the World (UW). In school, students use the interactive whiteboards and occasionally use ipads as a tool for a particular purpose. Parents are informed of safe digital use and healthy habits for young children at Parent Information Mornings.

Primary

In the Primary school, we follow the Common Sense Education Digital Citizenship curriculum which covers six key themes: Media balance & Wellbeing; Privacy & Security; Digital Footprint & Identity; Relationships & Communication; Cyberbullying, Digital Drama & Hate Speech; News & Media Literacy. This curriculum is co-taught by class teachers and our specialists computing teachers.
Children also learn about a range of E-safety-related topics through the PSHE curriculum (Jigsaw). During Digital Citizenship week, the profile of digital responsibility is raised greatly but it is also embedded into the computing curriculum where appropriate.

Senior
In the Senior school, children learn about many topics related to Digital Citizenship through the Living in the Modern World curriculum (taught discretely).
Yr 7 - Cyberbullying
Yr 8 - Sexting, Image sharing, Pornography
Yr 10 - Revenge Porn, Fake News and Critical Thinking
Yr 11- Online Gambling, Digital Footprint, Dark Web

Roles and Responsibilities:

Safeguarding Team

The school's Safeguarding team has overall collective responsibility for digital safety across the whole school.

DDSLs

EY DDSL: Alys Leighton Rahman
Primary DDSL: Jerome Marshall
Senior DDSL: Matthew Gibson

For specific sections of the school, each respective DDSL takes lead responsibility for digital safety by:

- Supporting the SLT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Heads of school, ICT manager and other staff, as necessary, to address any digital safety issues or incidents
- Managing all digital safety issues and incidents in line with the school child protection policy
- Ensuring that any digital safety incidents are logged on the appropriate online platform (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy
- Updating and delivering staff training on digital safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on digital safety in school to SLT and/or governing board

The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- At King's Bangkok, we use a range of filtering and monitoring software and tools including: Smoothwall, Juniper firewall, Gmail quarantine
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Monitoring the school network and email to ensure that any misuse or attempted misuse is alerted to the school Executive Principal and the DSL

All staff (including volunteers)

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use

- Working with the DDSLs to ensure that any digital safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents and carers

Parents are expected to:

- Notify a member of staff or SLT of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- Parent tips and guides - Common Sense Media
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Parents are kept informed about issues related to E-Safety and Digital Citizenship through weekly newsletters. They are also invited to parent presentations and workshops designed to help them support their children at home.

Cyberbullying

Cyberbullying is bullying which occurs though media and communication devices: these include mobile phones, and tablets. As a school, we will not tolerate cyberbullying and take all allegations seriously. We will invoke our Anti-Bullying Policy to deal with each case individually. Other staff members and parents will be informed as appropriate.

It includes the sharing of illegal material; the sharing of images of children and young people of an explicit nature; the sending of malicious communications to another person. It includes bullying that takes place outside school and can be reported via the usual channels to pastoral staff in school.

Youth Produced Sexual Imagery/ Image Based Sexual Abuse and Harrassement

Youth produced sexual imagery is when someone shares sexual, naked or semi-naked images of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops – any device that allows you to share media and messages. Youth produced sexual imagery may also be called:

- Trading nudes

- Sexting
- Dirties
- Pic for pic

Youth produced sexual imagery can be seen as harmless or consensual by young people but creating or sharing explicit images of a child or young person is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- Take an explicit photo or video of themselves or a friend Share an explicit image or video of a child, even if it is shared between children or young people of the same age
- Possess, download or store an explicit or video of a child, even if the child or young person gave their permission for it to be created

In the most recent guidance produced by the UK Council for Child Internet Safety, Sexting in Schools and Colleges Resource Pack, sexting is referred to as "youth produced sexual imagery".

We recognise that image-based sexual harassment constitutes digital sexual violence and requires immediate intervention. We know that these practices are extremely common. We aim to embed a culture within our community where sexual harassment and sexual abuse are not tolerated.

Child on Child Abuse

Child on child abuse can manifest itself in many ways and can include, but is not limited to, bullying, cyberbullying, sexting, gender-based violence and sexual abuse. It often manifests itself through the use of mobile devices and the internet. Child on child abuse is not tolerated at King's College Internationl School Bangkok and it should not be passed off as "banter" or "part of growing up". In the case of child on child abuse, our Safeguarding Policy and Anti-Bullying Policy should be invoked. Our Safeguarding Policy and this Digital Responsibility Policy set out the procedures taken by the school to minimise the risk of child on child abuse, and the Safeguarding Policy clearly states how allegations of child on child abuse will be investigated and dealt with.

Staff receive regular training in how to manage a report of child on child sexual violence and sexual harassment with the added guidance that they must not view or forward illegal images of a child.

We are committed to proactive work with students making the most of learning from Ofsted's review of sexual abuse in schools and colleges and wider research including "Understanding and Combatting youth experiences of image based sexual harassment abuse".

Artificial Intelligence

Artificial Intelligence (AI) is a swiftly advancing technology poised to transform various aspects of our lives, including education. This document delineates the principles governing the acceptable application of AI within our school community, guaranteeing benefits for both students and staff while upholding safety, privacy, and equity.

In relation to AI, King's Bangkok is dedicated to:

• Advocating for responsible and ethical use of AI technology in the school environment.

• Ensuring the integration of AI enhances the educational experience without compromising privacy or security.

• Cultivating innovation and creativity in using AI for educational purposes.

• Establishing explicit expectations for students, teachers, and staff regarding AI use.

Definitions:

• AI Technology: Any software or hardware system using machine learning, data analysis, or automation to execute tasks or make decisions without explicit programming.

Educational Enhancement

AI can enhance educational experiences, such as personalized learning, data analytics for performance improvement, and educational software. The primary objective is to enhance learning outcomes and foster academic success.

Privacy and Data Security

• Staff must refrain from sharing students' personal data with any AI systems. All data collected or generated by AI systems must be securely stored and used exclusively for educational purposes.

• Personally identifiable information (PII) must be safeguarded in accordance with relevant laws and regulations, such as the PDPA.

• Consent must be obtained from students and parents/guardians before collecting any personal data for AI-driven educational purposes.

Ethical Considerations

• AI systems must not perpetuate bias or discrimination. Efforts should be made to ensure fairness and equity in their design and use.

• Teachers and students should be educated about the ethical implications of AI technology and encouraged to discuss these issues in the classroom.

• Any use of AI that may infringe upon the dignity or privacy of individuals should be avoided.

Guidelines for Students

• Students should actively engage with AI as a supplement to their learning, not a substitute. AI can assist in research, data analysis, grammar and spell-checking, and even generating improvement suggestions.

However, it should never replace critical thinking, creativity, and problem-solving skills, which are core educational objectives.

• Students must be mindful of the ethical considerations surrounding AI usage. This includes appropriately citing AI-generated content, ensuring data privacy and security, and avoiding plagiarism by attributing AI-generated assistance in their work.

• Furthermore, students should view AI as a learning opportunity, seeking to understand the algorithms and processes behind AI tools, enabling them to make informed decisions about when and how to use AI in their academic pursuits.

• Students are expected to use AI technology responsibly, adhering to the school's code of conduct and this policy.

• Misuse of AI technology for cheating or academic dishonesty will not be tolerated. Refer to the updated academic honesty policy.

AI usage

Under the terms and conditions of most AI tools, users must be at least 18 years old to use some of them. ChatGPT allows users aged 13 or over to use the tools with parental permission. Therefore, primary students should not be using AI tools as it violates the service's terms and conditions. Children in Primary school will not engage with AI tools. Senior school students should only use AI in accordance with the terms of academic honesty policy.

Reporting Concerns

• Students should report any concerns regarding the use of AI technology that may violate this policy to a teacher or school administrator.

Guidelines for Teachers and Staff

Integration into Curriculum

• Teachers are encouraged to incorporate AI technology into their curriculum when suitable and beneficial for student learning.

• Training and professional development opportunities will be provided to assist teachers in effectively using AI in the classroom.

Monitoring and Accountability

• Teachers and staff members utilizing AI systems are responsible for ensuring compliance with this policy and applicable laws.

• They should report any technical issues or ethical concerns related to AI technology.

User accounts

All students in Year 3 and above will have access to Google Drive and students in Year 4 and will have email addresses created by the school. All students in key stage 2 or above will be issued with a login for the school network and will be given a password.

- Students must keep their password secret.
- Students must keep their own username and password secure and not share them with anyone else
- Students must log off when they have finished using a school computer or school device
- Students must never use a computer whilst logged on as another person.
- Students must observe academic honesty and any copyright restrictions in their research.

Classroom devices

Unsupervised primary school and EY students may not use devices in classrooms without permission. Senior school students are allowed to use devices in restricted areas at lunchtimes only which are monitored by duty staff.

Email

- Students must not use internet-based email services (such as Hotmail).
- Students may not send emails which appear to be either anonymous or from another person.
- Students may not send bulk emails (i.e. emails to more than five recipients) unless a teacher gives prior consent.
- Students must only use the school Google Workspace account when accessing Google services on the school network

Internet

- Network internet access at school is appropriately filtered. The school is mindful that this should not lead to unnecessary restrictions on learning, and any student who wishes to block/unblock specific sites should talk to their teacher.
- The school network may only be used for research related to academic subjects, individual study, co curricular activities, higher education or careers, i.e. for educationally beneficial tasks rather than recreational use such as games. Students may not use chat services at school unless this is sanctioned by a teacher and is for educational purposes.

Hacking

Hacking is illegal and is forbidden. This includes attempting to gain access to any file, function or network area which a student does not have permission to view or use. Students must not attempt to bypass monitoring software.

Rogue files

Students must not at any time have software or applications on the network (e.g. files ending in .exe, .com or files containing these, applications other than those installed by school). If students use compressed files, they must un-compress them before logging off.

Students must not use the network to store files which are solely for their personal recreation or files which cannot be accessed using software or applications available at school. Any external hard drives found to contain executable programs may be confiscated.

Offensive material

Students must not use ICT to view, send or store offensive material, including extremist websites which could incite hatred or violence. If such material is seen, discovered or viewed by a friend, it should be reported immediately to a teacher, preferably the student's form/house tutor.

Mobile phones

- Children in the EY and primary school are not allowed to have mobile phones in school.
- Students in Year 7 upwards may have a mobile phone which they must leave with their tutor during the school day. They may use this to contact parents at the end of the school day. They should only use their phone in the day if it is an emergency and they have their teacher's permission to do so.
- Students found with their phone during the day will have it confiscated and returned at the end of the school day to the parent or the child.
- Any teacher may confiscate a phone. If they do so, they should clearly tell the student:
    - why the phone is being confiscated;
    - when they can collect the phone again; and
    - where they can collect the phone from.

The phone should be placed in an envelope with the student's name and class written on, and the envelope stored in a secure drawer.

The school is not responsible if mobile phones are lost or damaged in school. It is the responsibility of the student and family to ensure the phone.

Taking, storing and publishing photographs, film and audio

Students must ask a teacher's permission before taking photographs at a school event or on the school site.

- Even when acting with permission, students should bear in mind the ethos of the school's Anti-Bullying Policy and must not take photographs and recordings of other students which:
    - might cause embarrassment or distress;
    - are associated with distressing or sensitive issues;
    - are unnecessarily intrusive;
    - are taken when a student would not expect their activities to be recorded or photographed; and/or

    - involve using a device which would enable a third party to take photographs or recordings remotely.
- Students must not share on social networking sites, blogs or in any other way photographs and recordings of other students taken at school, at school events or on school trips, without satisfying themselves that other students appearing in the photograph or recording have given or would give their consent to the sharing of the photograph. If a student is unsure, they should ask a teacher's permission before posting the photograph.
- If another student in the photo asks that it is not shared on social media, the student who has shared the photo must comply with that request or, if already shared, remove the photo from the social media site.
- Students must not share with third parties, such as publishers, journalists or web designers, photographs or recordings of other students taken at school, at school events or on school trips, without the permission of the school.

Personal computers and wifi

- In special circumstances, primary school and EY students may be able to use a personal device for preparing written work. If a student is allowed to use a personal device, they:
    - ensure that the laptop is only used when needed, eg, for written tasks;
    - take responsibility for the device; loss or damage of the device is not the school's responsibility; and
    - be reminded that using the device inappropriately will result in confiscation.

Students who have permission to use a personal computer as their normal way of working, may bring computers, tablet computers and mobile phones into school and may use them to access the school wifi network for educational purposes under the same conditions as they use school devices.

Internet access is only permitted using the school's wireless system and will remain filtered. All activity will be logged and any attempt to bypass such monitoring is not permitted.

The school reserves the right to access equipment at any time and/or put specific software on the equipment to bar the use of games or other non-academic usage.

No person other than the owner of the personal computer or a member of the ICT Department is allowed to use the personal computer.

Permission must be sought before using a personal computer with the school's network facilities, such as printers.

Printing

Students must not print unless given special permission by the teacher supervising them. Students must take care not to print excessive amounts of waste paper by printing unnecessary material.

If a file does not print, students should check that there is paper loaded in the printer. If it still does not print, they should cancel the print job from the queue and report the problem to a teacher.

Valuables

Securing electronic equipment that is brought into school remains the responsibility of the student, who must ensure that the owner's name is marked clearly on it.

The school strongly advises parents to take out insurance for any personal computers brought onto school premises.

Response to incorrect use

A breach of the provisions of this policy will be dealt with under the Promotion of Good Behaviour, policy, the Anti-Bullying Policy, academic honesty policy or the Withdrawal Procedure policy, as appropriate.

After consultation between staff and parents, we have upgraded our firewall to prevent students accessing various non-education centered sites on their devices at school. From now on, students won't have access to the below sites when connected to the school WiFi:

- Various gaming websites
- Social media applications including Discord, Instagram, Facebook and Line

As a result, the school's policy now reflects that students should not access these sites during the school day. We ask that parents ensure students do not have a VPN on their school devices, as these can be used to work around the firewall and this could encourage students to infringe the school's policy.

Students are not allowed access to their mobile phones throughout the day and are not allowed to hotspot to their personal devices or have a SIM card in their school iPads.

Digital citizenship agreement

All students in Y5-6 complete the Student Digital Citizenship Agreement Y5-6

All students in the senior school digitally sign to say they have accepted the Student Digital Citizenship Agreement Y7-13 including Smoothwall

Review and Revision

This policy will be periodically reviewed to ensure its effectiveness and relevance in the ever-changing landscape of digital technology. Necessary revisions will be made to reflect new developments and best practices.