KING'S COLLEGE INTERNATIONAL SCHOOL
BANGKOK

Reference number		**Policy name**	Acceptable Use Policy for Students: ICT at King's Bangkok

Person(s) responsible	WFO	**Date of next review**	July 2024

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	Students at King's College International School Bangkok ("King's Bangkok") are required to accept these rules as a condition of using school ICT facilities and will be reminded of them regularly. They apply to the use of all fixed and mobile technologies, whether on or off-site; networked or standalone; school or personal devices; and tablets or smartphones. All our students should act with kindness, good manners and wisdom at all times. Any violation of this policy should be reported to a teacher immediately.`

Approved by	SLT	**Date**	11/07/2023

Acceptable Use Policy for Students: ICT at King's Bangkok

Summary

Students at King's College International School Bangkok ("King's Bangkok") are required to accept these rules as a condition of using school ICT facilities and will be reminded of them regularly. They apply to the use of all fixed and mobile technologies, whether on or off-site; networked or standalone; school or personal devices; and tablets or smartphones.

All our students should act with kindness, good manners and wisdom at all times. Any violation of this policy should be reported to a teacher immediately.`

1 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 never use a computer whilst logged on as another person.
- Students must observe academic honesty and any copyright restrictions in their research.

2 Classroom devices

Unsupervised students may not use devices in classrooms without permission.

3 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 should be kind and polite in all online communication. Any rude or bullying behaviour will be dealt with using the school's Behaviour, Rewards and Sanctions Policy, Peer on Peer abuse and Anti-Bullying Policy.

4 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.

5 Monitoring

Students should be aware that any use of the school network will be monitored to ensure appropriate usage. This includes the analysis of internet sites visited, even if they are blocked.

King's Bangkok has a robust system for monitoring internet searches and blocking websites and links which are inappropriate for students and staff to use while on the school site. The system is managed by the ICT department.

6 Online safety

Students are taught through PSHE to manage their digital footprints, respect their own privacy and that of others, and 'think before they post'. They are aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Students should always report concerns to a parent or trusted teacher at the school.

7 Cyber-bullying

The school recognises that whilst mobile devices and computers are a source of education, communication and entertainment, some adults and young people may use these technologies to harm children. The harm might range from sending hurtful or abusive messages and emails, to enticing children to engage in sexually harmful conversations online, webcam filming, photography, sexting or face-to-face meetings. These technologies may also be used by those who wish to radicalise vulnerable children for their violent purposes.

Students receive guidance on cyber safety and bullying through our PSHE and computing programme. Student use of social networking sites, texts and emails should not be hurtful to students or staff, here or elsewhere, neither should it bring the school's name into disrepute.

Cyberbullying, that is, using the internet, mobile devices, social networking sites or other online mechanisms to deliberately upset someone else is treated as seriously as any other type of bullying and is managed through our anti-bullying procedures.

Issues such as sexting are addressed in the safeguarding policy, in PSHE lessons and in regular workshops for students and parents.

Student resilience is encouraged so that students can identify risk and protect themselves and their peers. If a student feels that they or another person have been teased, bullied or threatened, they should report this to a trusted teacher or parent.

8 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.

9 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.

10 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.

11 Mobile phones

- Children in the pre-prep and Junior school are not allowed to have mobile phones in school.
- Students in Year 7 upwards may have a mobile phone which they must keep switched off in their bag throughout the 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 in Year 6 and below 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.

12 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.

13 Personal computers and wifi

- In special circumstances 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.

14 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.

15 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.

16 Sanctions

A breach of the provisions of this policy will be dealt with under the Promotion of Good Behaviour, policy, the Anti-Bullying 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.

All policies are reviewed regularly and are subject to change.