Acceptable Use Policy

From an early age, students have access to many forms of technology in school. We try to keep controls and restrictions to a minimum, whilst still retaining a strong level of safety and security. Educating children to respect technology and to understand their responsibilities is key to creating effective, safe users, and each student demonstrates this by agreeing to the guidelines within the Student Acceptable Use Agreement in **Appendix**

The use of the school network and Internet must be in support of and consistent with the educational objectives of the school. Transmission of any material in violation of any Thai law or school rule is prohibited. Use for political lobbying is also prohibited. The school network and access to the internet should only be used in support of learning or for officially sanctioned tasks.

Access
Bangkok Prep encourages an anytime, anywhere access policy, but as with any shared resource the user carries a great deal of responsibility for using the resource sensibly. Therefore, inappropriate use, including any violation of these conditions and rules, may result in cancellation of an individual's access to the ICT resources of the school. The school will determine appropriate use and may deny, evoke, suspend or close any user account at any time based upon its determination of inappropriate use by an account holder or user.

Monitoring
In order to make determinations on whether specific uses of the network are inappropriate, the school reserves the right to monitor;
- File server space,
- Web site logs
- Laptops or portable devices connected to the network infrastructure
- Other uses of the school computer networks or resources including email.

Network Etiquette
All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
- The school network resource or internet access should not be used for activities which do not relate to learning. If a student are in any doubt, they should seek advice from a teacher or the Head of ICT.
- The school network resource or internet access should not be used to download offensive, pornographic or copyright protected material. To do so could result in the removal of access rights or other appropriate sanctions.
- The network should not be used in such a way that would disrupt the use of the network for other users.
- All information accessible via the network should be assumed to be private property. Files belonging to others should not be altered, deleted or moved.

- Students should be polite and should not become abusive when messaging others. The IT facilities should not be used to engage in bullying or offensive activities.
- Appropriate language should be used and swearing, vulgarities or any other inappropriate language should be avoided.

Electronic mail (e-mail) is not guaranteed to be private. People who operate the system in school have access to all mail.

Use of any information obtained via the Internet is at the user's own risk. The school specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. All users need to evaluate the source of any information they obtain, and consider how valid that information may be. Guidance on how to evaluate online sources is offered in ICT lessons.

We expect all users of the internet to be a critical user of the information they identify as useful to them.

Use of Social Networking Sites

Bangkok Prep believes it is important to contribute to the holistic development of a citizen living in a fast changing and unpredictable world. It is apparent that for a citizen to enjoy success in such an environment it is likely they will need to possess a number of skills including those of being an independent learner. The use of social networking tools are becoming increasingly important for independent, lifelong learners as well as for professional networking and for this reason the school integrates the use of these tools into its teaching and learning processes whenever appropriate. Bangkok Prep recognises the role that social networking tools such as Facebook, MySpace and Twitter may play in the future social and professional lives of our students. We are also aware of the contribution that these or similar tools can offer to support learning. These tools are considered to be learning networking tools rather than social tools.

However, the School is mindful of the potential that, for some users, the social element can be prominent. In order to educate our students as to the potential pit-falls of these tools the use of these networking tools are not allowed for tasks unrelated to learning or school work. The use of these tools should only be as a result of obtaining permission from teachers or appropriate school support professionals.

Plagiarism

Data downloaded or copied and pasted from the Internet should not be passed off as the student's own work for any purpose. This activity is known as ***plagiarism*** and plagiarising material from another source could affect the assessment mark for a candidate.

- Any student involved in such activity for an internal piece of work is liable to be suspended.
- Any student involved in such activity for a piece of work for an external examination will be reported to the examination board.
- Any work must be the work of the candidate or acknowledged as the work of others.

Security

Security on any computer system is a high priority especially when the system involves many users. *Users must never allow others to use their network password*. Users should also protect their password to ensure system security and their own privilege and ability to continue to use the system.

If a student feels that they can identify a security problem on a network, they must notify a system administrator or a teacher. They should not demonstrate the problem to other users.

Students should not use another individual's account and should not attempt to log on to the network as a system administrator. Any attempt to do so may result in immediate cancellation of user access. Any user identified as being a security risk to the network may be denied access to the network.

Vandalism and Harassment

Vandalism and harassment will result in cancellation of user access to the network and internet resources. Vandalism is defined as any malicious attempt to harm, modify or destroy data (belonging to) of another user.

Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unsolicited and unwanted digital communication of any form.

Encountering Controversial Material

Our policy encourages the appropriate use of the network and internet access. But in so doing the Bangkok Prep acknowledges that users may inadvertently encounter material which is controversial and which others may consider inappropriate or offensive. However, on a global network such as the Internet it is impossible to control effectively the content of data and an industrious user may discover controversial material. **It is the user's responsibility not to initiate access to such material and to inform teachers or an appropriate adult if they inadvertently encounter such material.**

Penalties or Sanctions for Improper Use:

Any user violating these rules or applicable Thai laws is subject to loss of network access or other school disciplinary options.

Review of Policy

This Acceptable Use Policy will be the subject of regular review.

BANGKOK PREP
Bangkok International Preparatory & Secondary School
Est. 2003

Primary Campus
23 Sukhumvit 53, Vadhana, Bangkok 10110

Secondary Campus
77 Sukhumvit 77, Vadhana, Bangkok 10110

Phone: 02-700-5858   **Email:** info@bkkprep.ac.th   **Web:** bkkprep.ac.th

Appendix 1 Student Acceptable Use Agreement

Internet Access

- I will only access the Internet for learning and school related activities and if I have permission from a teacher.
- If I accidentally access a website that is unsuitable or inappropriate, I will immediately click 'back' and tell a teacher.

Communication

- I will use polite and sensible language when using the Internet. If I receive a message that is unpleasant, I will inform a teacher immediately.
- I will access websites, social networking sites or chat rooms only for learning and school related activities or unless given express permission by a teacher while in school and I will always ask permission from a teacher before accessing my personal email account.

Security

- I understand that downloadable games, videos or other material can contain viruses. I will not download or install anything on to a school computer.
- If I have a password to access the network, a website, or an email account, I will keep it private and share it with no one (other than my teacher or parent if required).

Safety

- I am aware that anything I do or say on the Internet could be seen by others, including personal information, which might put me at risk.
- I will never give my full name, address or phone number when on the Internet or in an email.

Hardware

- I will treat ICT equipment responsibly, ie using it appropriately, safely and returning after use.

Privacy

- I will respect the privacy of others and will never open or tamper with another person's file or folder.
- I will only use my own login details and password.
- I understand that all activity on the school network is monitored and logged.

Student Name and Class	
Student Signature	

Parent Name	
Parent Signature	