Pupils' Acceptable Use Policy

Please read this carefully.

The school has provided computers / laptops for use by pupils, offering access to vast amounts of information and rich multimedia resources for use in studies and offers great potential to support the curriculum.

The computers / laptops are provided and maintained for the benefit of *all* pupils and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom.

Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

This Acceptable Use Policy is intended to provide a framework for such use of St. Constantine's International School's ICT resources. It applies to all pupils / students using the school's ICT systems and to others offered access to school's resources.

Responsible Internet Use
This Responsible Internet Use statement helps to protect pupils, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Internet access must be made via the user's authorised account and password, which must not be given to any other person
- The school's computer systems and internet use must be appropriate to the pupils' educational activity.
- The use of chat rooms, instant messaging, newsgroups and all social networking sites (e.g. Facebook, Myspace, Bebo, Twitter, Rate My Teacher to name but a few) is *strictly prohibited*, in accordance with the '*E-Safety Policy*'.
- On-Line, LAN or any other type of gaming is *strictly prohibited* unless appropriate permission has been given and is supervised by your teacher.
- The school ICT systems may not be used for private purposes, unless permission has been given.
- Only use the ICT equipment of educational purposes. Use for personal financial gain, gambling, political purposes or advertising is *not permitted*.
- Technology misuse including cyber-bullying, aggressive/abusive/offensive messages, photos and videos via SMS text messaging, email or social networking sites and any other anti-social behaviour is *strictly prohibited* and will not be tolerated.
- Pupils must report any unpleasant content, offensive messages, videos or pictures sent to them via SMS text messaging, email or social networking sites.
- The School will take all possible precautions to prevent access to unsuitable material. The use of filtering from our Internet Service Provider and in-house software cannot, however, entirely prevent access to internet sites that display objectionable material, or prevent unsuitable email contacts.
- If pupils discover unsuitable sites, the URL (address) and content must be reported to their teacher.

The school may exercise its right to monitor the use of the school's computer systems including network storage areas, access to web-sites, the interception of e-mail and to delete any inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery, video or sound.

Equipment

- Damaging, disabling or otherwise harming the operation of computers / laptops or intentionally wasting resources puts you and your work at risk.
- Protect ICT equipment from spillages by not eating or drinking when using these resources.
- Report any information on security violations to a member of staff.
- Report any physical damage to a member of staff.
- Protect assigned user passwords and other access keys from disclosure.

Email addresses

- Never publish your personal email address on any other website without authorisation.

- Pupils' should use the school's email address allocated to them during the school day. Student must not use school email account to register for social media purposes.
- Delete all spam, chain and other junk emails without forwarding or opening them.
- Only open attachments from emails if they come from a known and trustworthy source. Attachments can contain viruses or other programs that could destroy all files and software on your computer.
- Attachments (where authorised) must not be sent with email messages unless it is clearly stated on the email what the attachment is and the purpose for sending it.
- If you receive emails containing material of a violent, dangerous, racist or inappropriate content nature, always report such messages to your teacher and or to the ICT technical team.
- The sending or receiving of an email containing content likely to be inappropriate for schools is strictly forbidden.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then 'double delete' them by emptying recycle bin.
- Anonymous messages and forwarding of chain letters is not permitted.

Virus Prevention

- Never download files from unknown or suspicious sources.
- Attachments on emails should be saved on to the computer then scanned before opening, using the anti-virus software provided. Files that are downloaded must be saved to the computer's hard drive and scanned before opening.
- Always check files brought in on removable media such as portable hard drives, USB memory sticks or any other storage device with the anti-virus software provided and only use once satisfied they are clean of viruses.
- Where email applications act in an unusual way, such as multiple copies of the same message being received, or there is any suspicion that a computer is not operating as normal, technical support staff should be notified.
- Student must not run or install programs from own memory sticks or any other removable media without the permission of the technical support team.
- It is student's own responsibility to ensure personal home computers are protected with suitable virus protection software, malware software and have the latest security updates via the Microsoft website (Windows OS only).

Security

- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your data at risk.
- The school's computer system security must be respected; the downloading of programs or plug-ins is *strictly prohibited*.
- Software programs designed for compromising security are *strictly prohibited*. Examples of these tools include password guessing programs, cracking tools, key-gens or network probing tools.
- It is *prohibited* to examine, change or use another person's files, or user name for which they do not have explicit authorisation.

Content and copyright

- Copyright and intellectual property rights must be respected. This means no illegal downloads
- Ensure also that the school is not infringing copyright through any content published on the website.
- Pupils shall not publicise any confidential or personal information they find on a PC or laptop. This includes, but not limited to: financial information, databases and the information contained in them, personnel lists, computer software source codes and computer/network access codes in accordance with the Data Protection Policy.

Please read this document carefully. Only once it has been signed and returned will access to the school's ICT resources be permitted. If you violate these provisions, access to these resources will be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policies regarding school behaviour. For serious violations you may be temporarily or permanently excluded. Where appropriate, police may be involved or other legal action taken.

Pupils' Acceptable Use Policy once signed please return this slip to your teacher.

I have read this document carefully and understand the above. I agree to use the school's ICT facilities in accordance with this Acceptable Use Policy.

Pupil Name: _____ Signature: _____

I have read and understand the above.

Parent/Guardian Name: _____ Signature: _____