King's College
The British School of Madrid
Soto de Viñuelas

ICT: Acceptable Use Policy

This policy relates to the use of technology, including any devices which may be used for network, internet or email access (including Personal Computers, Laptops, Tablet devices, phones or games consoles), or the use of any internet or King's College system.

This policy applies to all at King's College including members of staff and students. For staff this policy constitutes part of terms and conditions for employment.

It applies to the use of technology on King's College premises and also any use, whether on or off the premises, which affects the welfare of others or where the culture or reputation of the organization are put at risk.

King's College Network

- Every person using computers connected to the King's College Network is allocated network file space to store personal work. Network file space must not be used for the storage of personal music, picture or video files.
- Do not give your account password to others, either inside or outside the organization.
- Respect the privacy of other users and do not attempt to access, modify or copy data or passwords belonging to others.
- Do not install, or attempt to install, software (e.g. games or other program files), or interfere in any way with hardware or network systems.
- Do not connect unauthorized hardware to any part of the King's College Network or telephone system.
- Connection of personal computers to the network requires permission from IT Services and is conditional on installation of appropriate anti-virus software, which must be kept updated.
- Exploitation of information available at King's College, especially for commercial purposes, is forbidden.

Internet Access

- The network also provides internet access, which is primarily provided for study by students or work related activity by staff. Reasonable personal use is permitted outside of normal working hours or study time provided it does not breach any other provisions of this policy. Controls are in place to prevent access to unsuitable material and control when students may access the internet. Access controls are also used to prevent access to internet services which could have a detrimental impact on the operation of our internet connection or internal network.
- Do not attempt to bypass or disable any security or control measures.
- Do not attempt to access pornographic or other unsuitable material.

- Comply with the guidelines for Social Network Sites.
- All internet access, and attempted access, is logged for monitoring and safeguarding purposes. Reports are available to managers and pastoral staff to allow scrutiny of individual internet use.
- Do not publish anywhere on the internet privileged information regarding any aspect of the organization, or anyone associated with the College, unless specifically authorized to do so.
- Do not post derogatory or inflammatory comments regarding the organization, or persons associated with the College, on any internet site, including Facebook, Twitter, etc. This applies to the use of College or personal computer equipment.
- Attempted access to blocked websites is logged. Should any user believe that access to a particular site should be allowed they may request that the website is unblocked. Such requests will be considered by the Head of ICT, in consultation with other senior management, and if considered appropriate access will be granted. Information is available on many different websites, prior to submitting an unblock request users should attempt to find the information they require elsewhere.
- The provision of privileged internet access to individual sites is not possible due to the detrimental impact such provision would have on system performance and support.

Email

- All staff are provided with a College email account. Email is provided for work related activity. Reasonable personal use is permitted outside of normal working hours provided it does not breach any other provisions of this policy. Email may be monitored to investigate or detect unauthorized use and ensure the effective operation of the system.
- Email carries the same legal status as other written documents and should be used with similar caution. Users have a responsibility to draft all emails carefully taking into account discrimination, harassment, defamation, and the need to maintain the reputation of the College. Do not send material which would or place the reputation of the College at risk.
- Do not send material that is libelous, indiscreet, offensive, or could jeopardize the welfare of others.
- Do not forward email which may contain sensitive information without permission of the sender.
- Always protect personal and confidential information about yourselves and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.
- Connection to VPN clients in any manner using a school device is strictly forbidden.
- Do not read, or attempt to read, anyone else's emails without their consent. This may constitute an offence.

- Do not open email attachments if you do not know the sender. Malicious attachments could place your computer, your email account, the College network or the reputation of King's College at risk.

Cyber-Bullying

- Cyber bullying is bullying which occurs by the use of electronic media such as mobile phones, cameras, email, and the internet. This could include any of the following:
    - Bullying by texts or messages or calls on the mobile phones
    - Use of mobile phone cameras to cause distress, fear or humiliation
    - Posting threatening, abusive, defamatory or humiliating material on websites
    - Hi-jacking email or other online accounts
    - Making threatening, abusive, defamatory or humiliating remarks in chat-rooms or other online facilities
- Cyber-bullying can be more intrusive than other forms of bullying because it can occur 24 hours a day, 7 days a week and may be almost impossible for a victim to escape. However perpetrators as rarely totally anonymous online and it is possible for the service provider (Mobile Phone Company, website owner or internet provider) to track the source. King's College deploys computer system logging and audit facilities which will be used to identify perpetrators. Cyber-bullying is against the law.
- Individuals will be held personally responsible for all the material they have placed on a website and for all material that appears on a website of which they are the account holder. Misconduct of this kind while away from King's College may give rise to disciplinary action if the welfare of others or the culture or reputation of the organization is placed at risk.
- King's College routinely monitors use of the internet and email for abuse and reserves the right to examine mobile phones, laptops or other devices where there is reason to suspect abuse.

Ownership of Systems and Programmes

- All computer programmes or systems developed or generated as a result of employment by King's College, or by the use of the College's hardware or software, will be the property of the College.

Disciplinary Action

- Any breach of this policy may incur disciplinary action in accordance with the policy appropriate to the individual. Serious breach of this policy may be considered gross misconduct.

Social Networking Sites

- Social networking sites such as Facebook provide dynamic new ways of communication with friends and family around the world. However, these sites can unintentionally expose far more personal details to the outside world than you would want. This could compromise your reputation, bring King's College into disrepute or provide opportunities for identity theft.

- The rapidly changing nature of these sites makes it difficult to give specific guidelines though the following are intended to help you avoid problems. Facebook is used as the example, however, the same principles should be applied to any other site that you use.
- Boarding staff and boarding students may make reasonable use of Facebook outside of work or study times.
- Ensure that your online profile only shows information you are comfortable to share with others, including personal details and postings.
- Do not publicise personal details regarding sexuality, politics or religion that you may regret at a later date.
- Do not post derogatory or offensive remarks regarding any person or organization.
- Do not post embarrassing or compromising photographs of yourself or others.
- Do not post messages which could incite or suggest unacceptable or criminal behavior.
- Set your Profile privacy settings so that your personal details and postings are only visible to your friends.
- Set your Profile so that only your friends and selected network members can find you.
- Do not agree to be friends with someone you do not know.

Applications

- Exercise caution when considering the use of an online Application. Signing up an Application often means you give the Application owner's permission to use your details and send messages or postings in your name. There are a number of malicious Applications available on Facebook, if in doubt do not sign-up to an Application. Do not assume that an Application is safe simply because a trusted friend has sent it to you; your friend may be the victim of a malicious Application.

Groups

- When considering joining a Group check which type it is. If it's a global group and open to anyone to join then look carefully at the postings before you decide to join. You will have no control over who reads your postings to this group. If the Group is closed there will be some measure of control by the Administrators and you will have to apply to join the group.
- If the title of a group is offensive to an individual, group or organization then do not join. Be aware that a group may be a pretending to be an official group, intended to deceive people into believing it is genuine. These groups are often used to slander or discredit others and risk prosecution if postings are libelous. When considering joining any Group look at the type of

postings on the group, before you become associated with it. If you are concerned with the type of postings within a group leave the group immediately.

- Be aware that if you decide to step up a Group you will be responsible for everything that is posted on that Group. It is recommended that any Group you create is closed to allow you to approve all members.
- Group Title and Description are visible to everyone with a Facebook account. If the title or description is defamatory towards an individual or group then it could be cause for legal action against the administrator and members.

Guidelines of Cyber-Bullying

Avoid being a Cyber-Bully

- Before sending a message to anyone, or posting a comment on a website about anyone, ask yourself if you would be happy to receive such a message, or see such a comment about yourself. If not then don't do it.

Dealing with Cyber-Bullying

- All the normal rules for dealing with bullying apply in accordance with the Anti-bullying Policy. If you are being bullied, or you know of someone else being bullied report it to the teacher, the house mistress, your tutor or a senior manager.
- Never reply or retaliate to bullying or abusive messages or images, or forward them to anyone. However they should be kept as evidence.
- Never give others passwords or passcodes to your mobile, email or other online accounts.

http://www.stoptextbully.com/ - preventing text bullying
http://www.chatdanger.com/ - general information on keeping online safe

Created and Reviewed by : CE May 2012	Policy Category: Behaviour / Welfare
Approved by EB: May 2012	Last Review: June 2015
Approved by School Council: June 2012	Next Review: June 2017