KING'S COLLEGE SCHOOL
WIMBLEDON

Internet & Electronic Communication: Acceptable Use Policy for KCS Employees

King's College School has a responsibility as a registered charity to ensure that all School resources are utilised correctly and not misused or abused. This includes electronic services such as Email and Internet access.

The School's Email & Internet Policies, which together with a third section concerning online communication between staff and pupils, form the **King's College School Acceptable Use Policy,** and were first formulated in 2002 by the ICT Development Group and governors, following wide consultation with all School employees, both teaching and non-teaching. This AUP includes some brief practical instructions for staff regarding email/phone/internet use, and advice about contact between staff and pupils. Further guidance on the personal use of social media in and out of school can be found in a separate **Social Media Policy**.

'Email' is taken to include all forms of electronic communication, including, for example, webmail, instant message and web forums. Use of the School's Internet and Email facilities, whether onsite, using wireless or via *KCS Remote,* will imply acceptance of the conditions of use laid down in these policies.

1. KING'S COLLEGE SCHOOL INTERNET POLICY

Purpose of Service and User Responsibilities

The Internet Service is provided primarily for King's College School use. However, it is acceptable for individuals to utilise this resource for personal use provided that usage is reasonable, sensible and managed by each employee responsibly, especially in respect of the time utilised when accessing the Internet. It should be noted that users of the Internet do not have a right to confidentiality or privacy when using or accessing King's College School communication tools. The Head of Computer Services monitors and reviews network logs maintained in order to ensure compliance with School policies. All users agree to such monitoring and reviewing of Internet access. KCS uses monitoring software to track the usage of the School's Internet service. This software records details of every web site visited, along with the relevant user name and date/time details, and produces regular reports for monitoring purposes. Misuse, or visits to sites of a dubious nature, will automatically be reported and dealt with in line with normal disciplinary procedures.

Any breach of this Internet policy or the associated Email policy will be taken very seriously and disciplinary action may result, which may involve summary dismissal in the most serious cases.

Users may not make their own provision for accessing the Internet from King's College School using resources other than those which have been provided through the School. Specifically, employees may not take out private subscriptions to Internet Service Providers and/or online services and use them on King's College School computer equipment unless this has been agreed in writing with the Head of Computer Services.

Users may not use the Internet in such a manner which might be prejudicial to the interests of King's College School or which may bring it or associated parties, such as parents or pupils, into disrepute. An example of this might be subscribing to a web site that

contains illicit or illegal material or by downloading and using a third party's copyrighted images unless explicitly permitted by the copyright owner.

Users who utilise the Internet must follow all existing School policies relating to confidentiality and anti-discrimination. Employees may not use the Internet to locate, download, access or otherwise investigate material of a nature which may cause offence to other King's College School employees on grounds of gender, race, religious belief, sexual orientation, disability or otherwise.

The downloading of software is strictly forbidden, in accordance with School policy, in order to minimise virus risks and to help ensure the network does not contain unlicensed software. This includes the downloading of games and screen saver software; where there is an educational need to make an exception to this policy please contact IT Support for guidance.

Employees may not use the Internet for inappropriate recreational use, such as games or gambling.

An employee may not knowingly use the Internet for any activity which is illegal under local legislation. Any employee inadvertently exposed to potentially illegal images whilst using the School Network *is obliged under Child Protection legislation* to report the location of those images to the School via the Head of Computer Services, and *must not* make copies or disseminate such images.

It is permissible to shop 'on line' on occasions where employees are working long hours. It should however be noted that you should avoid 'downloading' the retailer's software. King's College School cannot be held responsible for the security of any financial transactions, although the system is no less secure than a home based PC. Shopping should be restricted to items which do not fall into the categories described in the 'prohibited activities' section, especially items that are "obscene, pornographic or of an intimate nature".

It is essential that you do not divulge your user name or password to anyone else, as you alone are responsible for access and security of your Network Area. Computers should be "locked" when unattended (by pressing Ctrl-Alt-L or Ctrl-Alt-Del).

Prohibited Activities

Prohibited uses of the Internet at all times include, but are not limited to, viewing, storing, distributing or otherwise using the facilities for the following:

* Illegal activities (including any violation of copyright laws)
* Threatening, abusive, harassing or discriminatory behaviour
* Slanderous or defamatory purposes
* Obscene, suggestive or intimate messages or offensive graphical images or pornographic materials
* Activities that will incur a cost to the School without prior proper authorisation
* Chain letters through Email
* Private, commercial activities for profit making purposes
* Malicious damage
* Inappropriate political, religious or recreational use

Security and Access Considerations
King's College School is entitled to make provision to protect itself and its computer systems, web sites, pupils and employees from external or internal security threats, real or potential.

Examples of security measures which may be deployed include but are not limited to the following examples: Firewalls and Proxy Servers to block outgoing/incoming Internet traffic; Anti-virus software; Access control software (typically restricts access to specific web sites); measures to prevent the downloading of software; restriction of potentially harmful software scripting or elements.

The School currently subscribes to a filtered service from its Internet Provider. Whilst access to the Internet is generally not further restricted by the School for staff who are provided with the Internet, King's College School may block access to known sites which contain or are believed to contain illegal, pornographic or otherwise offensive material (for example sexually explicit; web-based chat; criminal skills & hacking; drugs, alcohol & tobacco; gambling & games; personals & dating; usenet news; violence & weapons). This is at the discretion of King's College School and the School is under no obligation to discuss the merits of otherwise of its decisions, or to advertise them.

King's College School's computer systems and resources are the property of the School, or are managed by the School, and are to be used in furtherance of the School's aims. Accordingly, King's College School reserves the right, without further notice, to monitor employees' use of any school computer systems or network resources including the use of Internet services. All communications and activities on the system cannot, as previously stated, be presumed to be private. Individuals who use this equipment are bound by this policy.

Users of the Internet should be aware that many web-sites record details (sometimes surreptitiously) of who visits them, and that access to the Internet could leave a record of activity on the PC itself.

The School reserves the right to withdraw the Internet without notice in the event of a suspected security violation requiring immediate investigation or where it otherwise believes that the King's College School Network and/or computer systems are at risk.

Support Considerations
The Internet is provided to enable access to the World Wide Web and this is the only Internet activity which is explicitly supported other than the use of Internet Email which is provided separately through the School's Email system.

The performance of the Internet is subject to its vagaries and is not under the control of the School. The School has made provision to use reliable and reputable Internet Service Provider(s) and will liaise with them over general problems.

2. KING'S COLLEGE SCHOOL EMAIL POLICY & GUIDELINES

Introduction
The purpose of this policy is to ensure the proper use of the Email system. Everyone who has access to Email is responsible for adhering to this policy, to ensure that it is operated within a proper legal framework and that it is used responsibly, effectively and for approved purposes only.

This policy is therefore set with the objective of making optimum use of the possibilities of communication by Email particularly for messages sent within the School, whilst at the same time avoiding the erosion of its value by overloading some individuals with Email correspondence.

Excessive personal use of the Email system has an adverse effect on its operation to the detriment of genuine users and is not acceptable.

King's College School aims to protect personnel from harassment or offence of inappropriate material or text.

It is important to have in mind that for legal purposes an Email message is not like a phone call, but is a recorded document (whether hardcopy or disk/network memory) and is discloseable in legal proceedings or to authorities, such as the Inland Revenue. You should also note that all Email messages sent or received by the King's College School Email system are the property of King's College School, and users should not expect personal privacy when using the Email system. The Head of Computer Services is authorised to monitor Email messages and network logs so as to ensure compliance with School policies. All users agree to such monitoring and reviewing of Emails.

Any breach of this Email policy or the associated Internet policy will be taken very seriously and disciplinary action may result, which may involve summary dismissal in the most serious cases.

Policy

Personal Emails: Whilst users of the Email system may send and receive personal messages internally and externally, this must not interfere with the user's work or the work of another user or be detrimental to the user's duties and responsibilities. Use should also not be excessive. The Email system should not be used for private commercial activities or to disclose, distribute or otherwise disseminate confidential information belonging to King's College School, or its associated or affiliated organisations.

Content: The content of all Emails must avoid any possibility of offence or harassment of a sexual, racial or religious nature, whether explicit or implicit, and must be written using only vocabulary acceptable for professional communication in the workplace.

Confidentiality: Confidentiality is not guaranteed. Any message sent or received may be accessed by colleagues other than the individual to whom it is sent, whether by accident (e.g. a computer left logged on) or design (e.g. an Email may need to be opened to diagnose connectivity problems). Messages cannot therefore be regarded as private or confidential. Personal messages should be written remembering this possibility for third parties to review the content. In the case of external (Internet) Email, there is no inherent security at all and such messages can potentially be intercepted and read by third parties without our knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium.

File Attachments: To avoid the possibility of any inappropriate material being copied down onto the King's College School Network, and to reduce the risk of virus infections, it is an absolute ruling that file attachments to Email messages, whether they be images, text or spreadsheets, may only ever be downloaded if they come from trusted sources (that is, from a correspondent whom you know) and are not of an inappropriate nature. Under no circumstances may attached executable program files be opened. Instead, such messages should be forwarded to the IT Support Team for advice. Executable files include those which end in the following suffixes: .EXE, .COM, VBS .SCR, game.exe, and screen.scr.

Chain Letters/Jokes: Chain letters and jokes are not an appropriate use of School time and resources and may unwittingly cause offence. If received they should not be forwarded and should be deleted from the network.

Virus Hoaxes/Warnings: Messages from external parties, which warn of viruses, must not be distributed or passed on. In practice most of these messages are simple hoaxes. However, in all cases they should be forwarded to IT Support for advice and then deleted from your Inbox.

Non-School Email Systems: All Email correspondence pertaining to King's College School must be distributed using the King's College School Email system. It is not permissible to use private Email systems and accounts (e.g. AOL, Hotmail, ISPs and others not cited) for School business.

Guidelines

Addressing Email

a) Check Carefully: Careful proofreading of addressees before sending will avoid common mis-addressing errors, e.g. the incorrect use of 'Reply All' vs. 'Reply' icons.

b) Principal Addressee: As well as entering the principal addressee into the address box on the Email header, the message should have a text heading "Message to xxxx" or be headed, "Dear xxxx" to make it clear who the recipient is and who is expected to respond. CCs would then only be copied for information.

c) CC Lists: As anyone would consider carefully the appropriate addressee and copy list for a memo or letter, so the same care should be given to addressing an Email. In particular multiple CCs of an Email should be avoided. Analyse carefully whether there is real and effective purpose to either copying the information or soliciting input from each and every person copied. *Do not* use CC lists for emails to groups of parents; such communications should be sent through the appropriate channel using the system described elsewhere in the Staff Handbook. **You are asked to take special care to respect the privacy of recipients such as parents by not using lists of email addresses in the 'To' or 'CC' boxes.**

d) BCC lists: Whilst there are appropriate uses of BCC with emails sent to third parties, its use can be a very bad idea for internal messages when knowledge of the sharing of communications between colleagues is withheld from one or more parties, since emails can be forwarded and the secrecy subsequently unmasked. Issues of trust between colleagues can arise when messages assumed by some to be private are shared in this manner, and so blind copying between colleagues is generally to be avoided.

Mass Emailing

Mass-mailed messages may only be sent for School purposes and may not be used to broadcast personal messages of any kind. Further, services/goods of third parties may not be advertised or recommended via Email.

Sending Document/Spreadsheet Attachments

Email may be used to distribute memos or other document attachments. However, large file attachments, defined as greater than 10 MB, may not be distributed (in general most documents and spreadsheets are well within this limit). IT Support can provide advice on the distribution of large files

e.g. by using shared areas.

3. ONLINE COMMUNICATIONS BETWEEN STAFF AND PUPILS

The GTC Code of Conduct for the teaching profession states that registered teachers must *establish and maintain appropriate professional boundaries in their relationships with children and young people*.

At KCS, we interpret this boundary to mean no contact with pupils on social networking sites (except for clear educational purposes e.g. *Moodle*) and minimal contact on email and telephone.

Some brief practical instructions for staff regarding email/phone/internet use:

1. Be alert to the way in which pupils can use these media to bully others, both in and out of school, but do not take sole responsibility for dealing with allegations of cyber bullying or other serious misuse yourself: report promptly up the line, as appropriate in the circumstances, so that an appropriate response to the allegations can be planned and implemented.

2. When using on-line resources and/or encouraging pupils to do so, assess the risks to pupils (e.g. is there access to chat rooms?) and take steps to minimise those risks (including providing any necessary guidance to pupils about how to use those resources safely).

3. If registering pupils on sites, be very careful about what data you provide – if personal data is requested (whether of pupils or parents), the safest thing to do is to get the informed consent of those people first, before you provide it to third parties.

4. Be mindful generally of what you do with information about others – who you send it to, how you use it, where you store it etc. The Data Protection Act is very wide-ranging, so familiarise yourself with the School's DP Policies (D13.5-7).

5. Take great care about your own use of email/mobile phones/social networking sites. Once emails, texts, comments on Facebook etc. have been sent, you have no control over them and they may well be seen by people other than the intended recipients and/or taken out of context. In short, think before you send. Another good test to apply is whether you would be completely comfortable with, say, a colleague seeing your correspondence.

6. Do not disclose or use personal email addresses and mobile phone numbers with pupils so far as possible. Similarly, avoid interacting with pupils on social networking sites, and reject online 'friends requests' from them.

7. Restrict use of email (and of mobile phones, if it is necessary to communicate via mobile phones) to school business.

8. Establish clear guidelines with your pupils about what is and is not appropriate when it comes to their use of electronic media, both with you and with others, in accordance with school policies and procedures. In particular, the Staff Student policy (D08.6) has some useful general guidelines on conduct with pupils. Any closed, unmonitored, communication with pupils is a potential risk.

9. Be aware that your role comes with particular responsibilities, and ensure that you are familiar with the **School's Social Media Policy**, which applies regardless of whether the media is accessed using the equipment belonging to the School or otherwise.
   You must adhere to the School's strict approach to the use of social media by King's staff for both business and personal purposes, whether during normal working hours or otherwise.