KING'S COLLEGE SCHOOL
WIMBLEDON

Acceptable Use Policy for Staff – ICT at King's

The Corporation of King's College School

King's College School, Wimbledon

King's College Junior School, Wimbledon

Wimbledon Common Preparatory School

JASR August 2018

Staff Acceptable Use Policy: ICT at King's

Internet & Electronic Communication: Acceptable Use Policy for Staff

King's College School ("the 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.

This policy comprises three sections:

1. Internet use policy
2. Email policy
3. Communication between staff and pupils.

This policy should also be read in conjunction with the following policies:

- Staff code of conduct
- Guidance for Staff on taking photographs or video recordings of pupils
- Social media policy
- Data protection policy
- Information security policy

The school's approach follows the statutory guidance as outlined in Annex C of the DfE document *Keeping Children Safe in Education (Sept 2018)*. Staff must be alert to the use of social media for cyber bullying and on-line radicalisation, and need to be aware of the Prevent duty as part of their safeguarding responsibilities. More details can be found in the Anti-Bullying Policy and sections 12 & 14 of the Safeguarding Policy.

In this 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 remote desktop acceptance will imply acceptance of the conditions of use laid down in this policy.

1. **Internet use policy**

1.1 **Purpose of Service and User Responsibilities**: The Internet Service is provided primarily School business. 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 spent when accessing the Internet for personal business.

1.2 Monitoring: Staff using the internet at school on the school systems do not have a right to confidentiality or privacy. The School has a robust system (Smoothwall) for monitoring Internet searches and blocking websites and links which are inappropriate for pupils and staff to use while on school site. The system is managed by the ICT department and monitored by the heads of section, Deputy Heads (pastoral) and the bursar. To ensure that flaws and gaps in the system do not arise, the firewall is challenged on a termly basis by members of the safeguarding team.

The monitoring software tracks the use of the school's internet and the Head of Computer Services and the Deputy Heads (Pastoral) monitor and review network logs maintained in order to ensure compliance with school policies. This includes the remote scanning of computer monitors, the checking of files and emails and the analysis of internet sites visited. 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. In using the school network, users agree to such monitoring and reviewing of internet access.

1.3 Private subscriptions or recreational use: Users may not make their own provision for accessing the Internet from 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 school computer equipment unless this has been agreed in writing with the Head of Computer Services. Employees may not use the Internet for inappropriate recreational use, such as games or gambling.

1.4 Bringing the school into disrepute: Users may not use the Internet in such a manner which might be prejudicial to the interests of the 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.

1.5 Downloading software: 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.

1.6 Unlawful use: An employee may not knowingly use the Internet for any activity which is unlawful under the law of England and Wales.. Employees may not use the Internet to locate, download, access or otherwise investigate material of a nature which may cause offence to pupils or other employees on grounds of gender, race, religious belief, sexual orientation, disability or otherwise.

1.7 Shopping online: 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".

1.8 Security: 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). Should a personal device, which has been used to access school emails or data, be lost or stolen, the loss or theft must be reported to the Head of Computer Services. Staff should ensure they are familiar with the ***information security policy*** which gives detailed guidance on password protection and security.

1.9 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

1.10 Safeguarding: Any employee inadvertently exposed to images depicting the abuse of children whilst using the school network must report the location of those images to the school via the Head of Computer Services, and **must not** make copies or disseminate such images. Any safeguarding issues arising out of the use of the school network by a member of staff will be dealt with under the ***Safeguarding policy***.

1.11 Security and Access Considerations: The school has in place 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, the 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).

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.

2. EMAIL POLICY & GUIDELINES

2.1 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, that email is used responsibly, effectively and for approved purposes only.

This policy is intended to provide guidance to staff on communication by email particularly for internal correspondence. For example, excessive personal use of the school email system is not acceptable.

2.2 Status of email communication: Staff should always bear in mind when communicating by email that in law, an email is a document disclosable in legal proceedings. All email messages sent or received within the school email network are the property of the 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.

2.3 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 of email for personal matters must 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 the school or corporation.

2.4 Content: The content of all emails must not contain 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.

2.5 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 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 and using the processes set out in the Information Security Policy.

2.6 File Attachments: To avoid the possibility of any inappropriate material being copied down onto the school network, and to reduce the risk of virus infections, file attachments to email messages, (whether they are 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.

2.7 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.

2.8 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.

2.9 Use of external email systems for school business: All email correspondence pertaining to school business must be sent using the school email network. It is not permitted to use private email systems and accounts (e.g. AOL, Hotmail, ISPs and others not cited) for school business. Staff who need to access the school network when off site should contact the IT helpdesk for advice on remote working.

2.10 Guidelines for sending email:

<u>Addressing email</u>

a) Check Carefully: Careful proofreading of addressees before sending will avoid common 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 portal. **You must 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. GUIDANCE FOR STAFF USING COMMUNICATION ONLINE AND USING ONLINE LEARNING RESOURCES

3.1 **Cyber-bullying:** Be alert to the way in which pupils can use these media to bully others, both in and out of school. If you suspect cyber-bullying or a case of cyber-bullying is reported to you, you must follow the procedures set out in the safeguarding policy. 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. Staff should make sure pupils understand the provisions in the ***Acceptable Use Policy, Pupils – ICT at King's***.

3.2 **Online learning resources:** 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. If registering pupils on sites, research the data you are required to provide beforehand. If personal data is requested (whether of pupils or parents) you may need to ask the parents for consent to register the child.

3.3 **Data protection:** Any communication that contains personal data will governed by current data protection legislation. Make sure you are familiar with the data protection policy and the information security policy both of which contain detailed guidance on how to keep personal data secure. Photographs and video recordings are personal data. Staff should not take photographs or video recordings on their own devices and should ensure they are follow the ***guidance for staff on taking photographs or video recordings of pupils***.

3.4 **Social media:** Take care when communicating via email or posting on social media in a personal capacity. Once email has been sent or a message posted, you have no control over who can view it and it may be shared with people other than the intended recipients and/or taken out of context. Be aware that your role as member of staff at a school comes with particular responsibilities. 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 staff for both business and personal purposes, whether during normal working hours or otherwise.

3.5 **Communicating with pupils**: The GTC Code of Conduct for the teaching profession states that registered teachers must e*stablish and maintain appropriate professional boundaries in their relationships with children and young people*. The school interprets this boundary to mean no contact with pupils on social networking sites (except for clear educational purposes e.g. *Moodle*) and minimal contact by email and telephone. Do not disclose or use personal email addresses and mobile phone numbers with pupils. Similarly, avoid interactions with pupils on social networking sites, and reject online 'friend requests' from them. Restrict communication with pupils by email or mobile phone to school business.

4. CONSEQUENCES OF BREACH OF THIS POLICY

Any breach of this internet policy or the associated may result in disciplinary action and / or summary dismissal in the most serious cases. A serious breach of policy which may be a criminal offence may be reported to external agencies such as the police, for investigation.