ACCEPTABLE USE OF COMPUTERS (GIRLS) POLICY

SENIOR SCHOOL

Any large computer network is a highly complex system requiring a considerable amount of maintenance. The points below are designed to ensure that the network is always available and working at the appropriate times. All users of the network (whether using School computers, personal laptops or any other device that can connect to the School network by whatever means) are expected to use their common sense, the more general School rules and the law of the land. This policy also applies to any access to the internet or the School network using 3G, 4G, wireless or any other technologies whilst at School or under School control.

This Policy should be read in conjunction with the policies listed below:

E Safety Policy	Behaviour Policy
Use of Images Policy	

1. SYSTEM SECURITY

1.1 Girls are responsible for their individual account and must never allow anyone else to use it, even when they are present. Passwords should be of sufficient complexity and must never be divulged to another person. Anyone who is concerned that the security of their account may have been compromised in any way must talk to their Form tutor or contact IT Support. Swipe cards are allocated to individual girls and should not be shared. Sharing of swipe cards will be deemed a breach of the acceptable user policy. Lost swipe cards must be reported to IT Support immediately.

2. UNAUTHORISED ACTIVITIES

2.1 Girls should not attempt to go beyond their authorised access. This includes attempting to log in through another person's account, sending e-mails while masquerading as another person, or accessing another person's files in their directory. No-one must make deliberate attempts to disrupt the computer system or destroy data. Girls should also not attempt to deceive other external secure websites through the School network. Any deliberate attempt to 'hack' into the School's IT infrastructure or to deliberately evade or circumvent the School's firewall, for example by the use of a Virtual Private Network (VPN), will result in disciplinary action that may include Temporary or Permanent Suspension from the School.

3. SOCIAL NETWORKING SITES

3.1 Girls must not post personal information to social networking sites such as YouTube and Facebook or using apps such as Whatsapp, Imessage, Snapchat, Facetime, Instagram and Twitter if such information would allow others to find out details of where a person lives. Such services, used sensibly, can provide genuine opportunities for keeping up with friends, but everyone must be aware that other users may not necessarily be who they say they are. No-one must use such services to impersonate others, to send inappropriate or offensive images, nor to participate in any form of "cyber-bullying". Nothing must be posted on such services which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute.

4. E-MAIL

Girls are referred to the 'Guidelines for the Use of Email' – Section II

4.1 No indecent, obscene, offensive, or threatening language can be used, nor should anyone engage in personal, prejudicial, or discriminatory attacks. At all times, privacy should be respected concerning any messages sent and no messages should be re-sent or forwarded to others without permission. School emails should be checked frequently and unwanted emails deleted. Girls must use their School email addresses when emailing members of staff.

5. INTERNET ACCESS

5.1 Use of the School network is carefully filtered and recorded for Safeguarding purposes. Computers at School or other devices which can link to the School network or the internet whilst at School (or whilst under School control) must not be used to access material that is profane or obscene, that advocates illegal acts, violence, or discrimination towards other people, or encourages radicalisation or extremism. If inappropriate information is mistakenly accessed, the Form tutor or another teacher should be informed immediately. This action will protect girls against the accusation that the material was intentionally accessed. Girls must not plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were one's own. Copyright must be respected. The internet must not be used to download illegal software or, for example, pirated music, images or films. No software or programmes may be installed on any School computer without explicit permission from IT support.

6. DEVICES

6.1 The rules that apply to School computers also apply to girls' own devices when brought to School. Girls should ensure that any unsuitable material (as defined in the previous paragraph) is deleted before bringing it to School. Girls must not be allowed access to each other's devices. Technologies such as 3G, 4G and wireless should not be used to gain unfiltered web access, nor may girls employ VPNs to breach or circumvent the Firewall. If there is a suspicion that a girl has broken these rules, the Form tutor or System Administrator may remove the girl's device without warning, prior to an investigation taking place in conjunction with the Head of School.

7. RESPECTING RESOURCE LIMITS

7.1 Large files should not be downloaded or saved unless absolutely necessary. Girls should refrain from excessive use of Social Media platforms to send video footage or images. This also applies to the streaming of films or television via the School network as these activities can restrict others' use of the network. Girls should respect the age classification of films they are watching and games they might play.

8. PRINTERS

8.1 Printers at School must only be used by girls for the production of educational material related to legitimate educational or co-curricular activities at Kent College. Girls should consider the necessity of printing material in accordance with responsible environmental awareness.

9. PRIVACY

9.1 Girls should expect only limited privacy in the contents of their personal files on the School system or on their laptop if used to connect to the system. The three Heads of School, System Administrators, the Form tutor, and parents or guardians have the right at any time to require access to a girl's School directory or laptop. As a general rule, girls should not store anything which they would feel uncomfortable justifying in front of any member of staff or their parents.

10. SANCTIONS

10.1 When using the School's system, girls may think that it is easy to break the rules above without the risk of detection. However, whenever the network is used, an electronic trace is left that can subsequently be followed. Depending on the severity of the offence, one or more of the following sanctions may be applied if a girl is found to have broken any of the above rules:

A formal warning	Suspension of internet access
Device confiscation (phone, tablet, laptop, PC etc)	Formal School sanctions
Temporary or permanent suspension from the School	Suspension of computer system account

SECTION II

11. GUIDELINES FOR THE USE OF EMAIL

11.1 Email is a vital tool for effective communication and one which facilitates good management of the complex and fast moving environment of Kent College. However, there are limitations to its usefulness and dangers associated with thoughtless or inappropriate use of email. Further, the sheer volume of email traffic and the associated expectations of an immediate response can lead to it becoming a significant burden for members of the School community, drawing them away from important pastoral or academic responsibilities. One aim of producing this guidance is to reduce unnecessary email traffic, thus freeing staff to carry out their primary functions. **This document gives guidance for staff, girls and parents.**

11.2 **Necessity.** Is an email the most appropriate mode of communication? Would a meeting or phone call lead to a quicker resolution? Remember also that your email may be one of many being read by the recipient; are they going to have time to give it full consideration?

11.3 **Replying.** Email accounts should be checked regularly but bear in mind that people are busy; do not expect an immediate reply (if an immediate reply is needed, email is not the correct mode of communication). On receipt of an email that requires a considered response or the collation of others' views etc, send a holding email acknowledging receipt and giving your intended timeframe for a full reply. This could reasonably be a number of days, depending on the circumstances. Activate the 'out of office' function to inform senders if you are unable to reply.

11.4 **Content.** Avoid sending frivolous emails, particularly to multiple recipients. Never include derogatory or defamatory comments and consider how someone other than the recipient might interpret your email. Emails provide a written record: you have no control over who prints, forwards or stores them or for how long they are stored. Remember that the laws which relate to written communication apply equally to emails. These include laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, GDPR data protection, freedom of information and discrimination.

11.5 **Style.** Always include an informative subject line. Be concise and avoid branching out into a number of different issues. Be conscious of the appropriate level of formality and ensure good standards of spelling, punctuation and grammar; text speak is not appropriate. Make clear any action that is requested or required of the recipient. Include a signature which describes your role and gives appropriate contact details when emailing someone for the first time.

11.6 **Tone.** Email should not be used when you are trying to convey complex feelings or to explore emotive issues. Emails are easy to misinterpret and may cause offence where none was intended. Consider saving an email written when tired, frustrated or annoyed and reviewing it the next day. Do not use email to reprimand or chastise, nor to convey bad news of a serious nature to an individual unless there is absolutely no alternative.

11.7 **Confidentiality.** Be wary of including sensitive or confidential information in an email. Consider the content of an email carefully before forwarding to others or Cc'ing additional recipients in a reply. Be aware that some staff allow administrative staff to access their email accounts. Recipients should only be included on a 'need to know' basis. Use the Cc box judiciously and do not expect a reply from anyone who has been Cc'd. Staff must always use the Bcc field when emailing a group of parents.

11.8 **Courtesy.** Respect everyone's right to time away from work. Just because email is theoretically accessible at any time, do not assume that recipients will read your email late at night nor expect that they will reply. Remember that people have different working patterns; do not feel pressured to reply if you receive an email at odd hours.

A copy of this policy is available on www.kent-college.co.uk

This policy is reviewed regularly.

Last revised, SLT: February 2015
Approved by Education Committee: March 2015
Revised: June 2017
Full revision: May 2018
Approved by Education Committee: June 2018