



ACCEPTABLE USE OF COMPUTERS (PUPILS) POLICY SENIOR SCHOOL

This Acceptable Use Policy is intended to ensure:

- that pupils at Kent College will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

| | |
|----------------------|----------------------|
| Online Safety Policy | Behaviour Policy |
| Use of Images Policy | Anti-Bullying policy |

Pupils, parents and guardians should read this policy and sign the Computer Acceptable Use Agreement – see Appendix 1

1. SYSTEM SECURITY

- 1.1 Pupils are responsible for their individual school network/Microsoft 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 pupils 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 Pupils 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. Pupils 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 Pupils must not post personal information to social networking sites such as YouTube and Facebook or using apps such as WhatsApp, TikTok, Snapchat, 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. In addition, pupils should avoid posting videos and photos online when in school uniform and they must be very mindful of the school's reputation in their online behaviour.

4. E-MAIL

Pupils 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. Pupils 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 pupils against the accusation that the material was intentionally accessed. Pupils 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. OWN DEVICES

- 6.1 The rules that apply to School computers also apply to pupils' own devices when brought to School.
- 6.2 Pupils should take full responsibility for their own device and bring it to school ready charged. Kent College is not responsible for the security and safety of student-owned devices. The device should either be kept with the pupil or locked away. Responsibility for the security of the device resides with the individual pupil. Kent College is not liable for any device stolen or damaged on site. The school strongly recommends that any device brought into school is covered on a parent's home/other insurance.
- 6.3 Pupils should not physically share their devices with other students unless they have written permission to do so.
- 6.4 Pupils may not use their device to record, transmit or post photos or video of a person or persons on site, unless directed to do so and under supervision from a teacher. This includes the recording of online lessons. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a member of staff.
- 6.5 Technologies such as 4G/5G and wireless should not be used to gain unfiltered web access, nor may pupils employ VPNs to breach or circumvent the Firewall. If there is a suspicion that a pupil has broken these rules, the Form Tutor or System Administrator may remove the pupil's device without warning, prior to an investigation taking place in conjunction with the relevant Student Manager/Deputy Head..
- 6.6 Kent College reserves the right to inspect a pupil's personal device if there is reason to believe that the pupil has violated school policy, school rules or has engaged in other misconduct while using their personal device. Network filters will be applied to any connection to the internet, and pupils will not attempt to bypass them
- 6.7 The device may not be used to commit academic dishonesty on assignments or tests or for non-instructional purposes.
- 6.8 Whilst at school pupils should only access content on their device or internet sites which is relevant to the curriculum. Pupils should not bring inappropriate computer games or any other inappropriate materials to school on the device. Pupils should ensure that any unsuitable material (as defined in the previous section) is deleted before bringing it to School. Pupils should not access TV/Film streaming sites such as Netflix during the school day without permission. Should a member of staff allow pupils to access these sites, pupils should respect the age classification of films they are watching and any games they might play. Failure to do so will result in sanctions.

Pupils must comply immediately with teachers' requests to shut down their device, close the screen or put the device away.

- 6.9 Devices should be updated with the latest security measures, including antivirus and firewall software. Any intentional attempt by the student to bring on premises or infect the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorised data or information is in violation of the Acceptable Use policy and will result in disciplinary actions.

7. RESPECTING RESOURCE LIMITS

- 7.1 Pupils should be mindful that whilst the School's Wifi bandwidth is significant it is not limitless. Activities that require a significant upload or download of data should ideally not take place during lesson times as this may impact on the teaching and learning of others. k. **PRINTERS**
- 7.2 Printers at School must only be used by pupils for the production of educational material related to legitimate educational or co-curricular activities at Kent College. Pupils should consider the necessity of printing material in accordance with responsible environmental awareness and are encouraged to save files and materials on their own device.

8. PRIVACY

- 8.1 Pupils 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 Deputy Heads and pastoral staff, System Administrators, and parents or guardians have the right at any time to require access to a pupil's School directory or laptop. As a general rule, pupils should not store anything which they would feel uncomfortable justifying in front of any member of staff or their parents.

9. SANCTIONS

- 9.1 When using the School's system, pupils 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 pupil 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

10. GUIDELINES FOR THE USE OF EMAIL

- 10.1 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, pupils and parents.**
- 10.2 **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?
- 10.3 **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.
- 10.4 **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.
- 10.5 **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.
- 10.6 **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.

- 10.7 **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.
- 10.8 **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
Revised: May 2021
Approved by Education Committee: June 2021

Annual Computer Acceptable Use Agreement Academic Year

Pupil:

I have read and I understand the school's Computer Acceptable Use policy. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Print Name: Form/Year Group

Signed: Date

Parent / Guardian:

As a Parent or Guardian I have read this agreement. I understand that although Kent College employs the latest filtering and security technology no system can be 100% safe. I give my child permission to use the school computer system:

Print name:
.....

Signed: Date

The Computer Acceptable Use consent form must be signed by both pupil and parent/guardian on an annual basis. Without it your child's access to the school network will be withdrawn.