## Kent College Senior School

# Computer Acceptable Use Policy for Students

### Introduction:

The use of the latest technology is actively encouraged at Kent College but with this comes a responsibility to protect both students and the school from abuse of the system.

All students, therefore, must adhere to the policy set out below. This policy covers all computers, laptops, mobile phones and other electronic devices within the school, irrespective of who is the owner.

All students are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school. Access to the school network is provided for you to carry out schoolwork, on the understanding that you agree to abide by this agreement.

### The Policy:

#### 1. Personal Safety:

1.1 Always be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.
1.2 Do not send anyone your credit card or bank details without checking with a teacher.
1.3 Always inform your teacher or another member of staff if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
1.4 Do not tamper with, or remove, any cables that are attached to a school computer.
1.5 Always be yourself and do not pretend to be anyone or anything that you are not on the internet.
1.6 Do not arrange to meet with anyone you have met on the internet. People are not always who they say they are.
1.7 If in doubt ask a teacher or another member of staff.

#### 2. System Security:

2.1 Do not attempt to go beyond your authorized access. This includes attempting to log on as another person, sending e-mail whilst masquerading as another person, or accessing another person's files. Attempting to log on as staff will be dealt with severely. You are only permitted to log on as yourself.
2.2 Do not give your password to anyone else. If you do and they do something wrong whilst logged on as you, you will be held responsible. If you suspect someone else knows your password, change it immediately.
2.3 Your password should be changed at least once every six months. It should be at least 6 characters long and contain numbers as well as letters.
2.4 Do not make deliberate attempts to disrupt the computer system or destroy data by any method, including knowingly spreading a computer virus.
2.5 Do not alter school hardware in anyway.

2.6 Memory sticks or other USB devices may only be used on computers that have USB ports on the front or side of them. Do not try to insert them in the back of computers.

2.7 The school retains the right to inspect immediately on demand any USB device held on the school premises, including the right to browse and open any files, programs or data of any nature held on a USB device and the right to confiscate the device at any time without prior notice.

2.8 Do not knowingly break or misuse headphones, mouse devices or any other external devices such as printers or scanners.

2.9 You may use your own headphones only if there is a headphone socket on the front of the computer. Do not attempt to plug them into the back.

2.10 Do not attempt to connect to another student's laptop or device while at school. Establishment of your own computer network is not allowed.

2.11 Do not eat or drink whilst using the computer or place food or drink near the computer.

2.12 Do not email or play computer games during lessons without permission from a teacher.

2.13 Do not use Smartboards outside lesson times.

2.14 Computers in Form rooms should be used only with the permission of the Form Tutor and should not be used to play music or videos during break times or study periods.

2.15 Your ability to connect to other computer systems through the school network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.

## 3. Inappropriate Behaviour:

Inappropriate behaviour relates to any electronic communication whether email, instant messaging, blogging, texting, journal entries, or any other type of messaging or posting / uploading to the internet.

3.1 Do not use indecent, obscene, offensive or threatening language.

3.2 Do not post or send information that could cause damage or disruption.

3.3 Do not engage in personal, prejudicial or discriminatory attacks.

3.4 Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.

3.5 Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.

3.6 Do not post or send private information about another person, including their photograph, unless you have their written permission first.

3.7 Do not use the internet for gambling.

3.8 Bullying of another person either by email, texts or any type of instant messaging application will be treated with the highest severity.

3.9 Do not access material that is profane or obscene, or that encourages illegal acts, violence, or discrimination towards other people.

3.10 If you mistakenly access such material please inform your teacher or another member of staff immediately or you will be held responsible.

3.11 If you are planning any activity which might risk breaking the acceptable use policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff of the relevant subject must be consulted beforehand.

3.12 Do not attempt to use proxy sites on the internet.

3.13 Do not take a video or photo of another student or member of staff without their permission.

3.14 Do not attempt to access any form of social networking site during the school day or during Prep Sessions after school, whether using a school computer, a mobile phone or any other personal electronic device. Boarders may access certain age-appropriate sites at times agreed with the Boarding Staff.

3.15 Do not use a USB device to carry any software of any nature to or from school.

## 4. Email:

4.1 You should check your school email each day for new messages.

4.2 Do not reply to spam mails as this will result in more spam. Delete them and inform the Network Manager.

4.3 Do not open an attachment from an unknown source. Inform the Network Manager, as it might contain a virus.

4.4 All emails sent outside the school reflect on Kent College so please maintain the highest standards.

4.5 An email attachment limit of **10MB** has been set globally for students. If you require a larger limit please contact the Network Manager.

4.6 Avoid sending trivial messages or forwarding spam or chain mail.

4.7 Do not join mailing lists without the prior permission of the Network Manager.

4.8 Unless you are a Sixth Form School Officer, do not send mail to a distribution list. Consult a teacher if you wish to send a message to a large group of people.

4.9 If you receive an email sent to you in error, please inform the sender as soon as possible.

## 5. Plagiarism and Copyright:

5.1 Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the internet or anywhere else.

5.2 You should respect copyright and intellectual property rights. Breaking copyright law occurs when you reproduce a piece of work or a picture that is protected by copyright. If you are unsure whether or not you can use a piece of work or a picture, speak to your teacher or a member of staff in the Library first. You may need to request permission from the copyright owner. This includes music files and the copying of CDs and videos.

## 6. Privacy:

6.1 All files and emails on the system are the property of the school. As such, the school has the right to access them or to intercept emails if required.

6.2 Do not assume that any email or any other sort of message sent or posted on the internet is secure.

6.3 All network access, web-browsing and emails on the school system are logged and routinely monitored to ensure that the Acceptable Use Policy has not been broken. The IT team can, at any time, monitor what is happening on any computer screen.

6.4 If you are suspected of breaking this policy, your own personal laptop or device and mobile phone can be searched by staff with the permission of your parents.

6.5 The school reserves the right to search the internet for inappropriate material posted by students and to act upon it.

## 7. Software:

7.1 Do not install any software on the school system.
7.2 Do not attempt to download programs from the internet onto school computers.
7.3 Do not knowingly install spyware or any sort of hacking software or device.
7.4 Do not use school internet facilities to download or distribute pirated software or data, or to propagate any virus, worm, Trojan horse, or trap-door program code.

## 8. Sanctions:

8.1 Sanctions can vary depending upon the severity of the offence, from a warning or withdrawal of internet use, to suspension or expulsion from school. Any breach of any law may lead to the involvement of the police or any other relevant authority.

## 9. General and Best Practice:

9.1 Think before you print. Printing is expensive and consumes resources, which is bad for the environment.
9.2 Priority must be given to students wishing to use computers for school use.
9.3 Always log off when you have finished using a computer. Do not leave a computer unattended and logged on, even for a few minutes.
9.4 Always back up your work if you are not saving it on the school system. Work saved on the school system is backed up regularly, but be careful if you only have a copy of your work on a USB device, as files may become corrupted or damaged.
9.5 Students are responsible for housekeeping of their personal network area. Please remove any files which are no longer necessary. We would recommend that housekeeping on your personal area is carried out once a term.
9.6 Always save your work at regular intervals (every 10 minutes). This is particularly important when completing any examined work (for example, controlled assessments, coursework).
9.7 Avoid saving or printing large files (over 10mb, for example).
9.8 If someone makes you an offer on the web or via email which seems too good to be true, it probably is.
9.9 Observe health and safety guidelines – look away from the screen every 10 minutes to rest your eyes. Make sure your chair is positioned and adjusted correctly.
9.10 Be considerate and polite to other users.
9.11 Delete old emails regularly and empty your Deleted Items folder regularly.
9.12 If a web page that you feel you have a legitimate use for is blocked, please ask the Network Manager if approval can be given to unblock the page.
9.13 The internet can become addictive. If you feel you are spending too long on it, please ask a teacher or another member of staff for advice about whether this is safe.
9.14 If you are leaving the school permanently, please ensure that you have saved any files or email you want to keep on a memory stick to take home.

Access to your email and network accounts will be disabled when you leave the school and all files will be permanently deleted within one year.

9.15 If in doubt about any aspect of computer or internet usage, please ask a member of the IT support team or the Network Manager.

## 10. Laptops, Tablet Computers (such as iPads), Smartphones and other PDAs:

10.1 If you wish to use your own personal laptop or other device you can only connect it to the network via the student network service. When accessing the internet on your own device, it is highly recommended that you use the school's Wi-Fi network connection. The school accepts that some devices automatically connect through other networks, such as 3G. Please note that this AUP applies to all devices and connections used on the school site and that you have a responsibility to ensure that content stored or accessed on your own device is appropriate. If in doubt, or you require further information or help, please contact the Network Manager.

10.2 Your laptop or device must have adequate security protection. Up-to-date anti-virus software must be installed. Your laptop or device may be scanned periodically to ensure this is so. An inspection of your device may take place to check the suitability of your device. Do not attempt to use hacking tools.

10.3 Do not plug a network cable into any school network point except the ones provided for this purpose in the boarding houses and Tilley.

## 11. Mobile Phones:

11.1 Mobile phones may be brought into school on the clear understanding that they are switched off on arrival at school and kept switched off during the day. Girls in Year 9 upwards may use their mobile phones during break and lunch times. Mobile phones may not be used in the dining room.

11.2 If you need to use your phone for any reason, such as a change in travel arrangements, you must obtain permission from a member of staff.

11.3 Contravention of the rules applying to mobile phones may lead to the phone being confiscated. Confiscated mobile phones can be collected from reception at the end of the school day.

11.4 Mobile phones are the responsibility of the owner and should be kept locked in lockers or in the personal possession of the owner. The school accepts no responsibility for the loss of a mobile phone.

11.5 Girls may use mobile phones after school in Form rooms. Boarders may use mobile phones after school only in their dormitories with the consent of their roommates. They must not be used after lights out.

11.6 Mobile phones may be taken on trips out of school. The same conditions apply: they should be switched off throughout the visit but may be used when the trip has ended to confirm travel arrangements.

11.7 Mobile phones may be used during lessons for educational purposes with your teacher's permission.

11.8 Do not take photos or videos with a phone during lessons unless the member of staff has given permission.

11.9 Bullying by text message or any other messaging method will be treated in the same severe manner as any other form of bullying.

11.10 Do not attempt to hack into someone else's device via Bluetooth or any other method.

## 12. Music / Video players e.g. iPods

12.1 The use of such devices is banned during lessons unless the teacher has given permission.
12.2 Do not connect such a device to the school network or school computers.
12.3 Do not break copyright laws by illegally swapping or copying music or video files.

## 13. Other Electronic Devices:

13.1 The Acceptable Use Policy above covers all electronic devices such as laptops, iPads and mobile phones while they are being used on school premises.
13.2 Please note that none of these devices are covered by the school's insurance and the school accepts no liability for them.
13.3 All devices should be security marked and kept locked away where possible. This also applies to other items such as digital cameras, personal DVD players and iPods.

## 14. **Swipe cards**

14.1 Swipe cards are allocated to individual girls and should not be shared. Sharing of swipe cards will be deemed a breach of the acceptable use policy.

14.2 Lost swipe cards will be replaced once, but thereafter will incur a charge.

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