Technology & Acceptable Use Policy for Boys

Introduction

The use of technology is actively encouraged at Summer Fields, but with it comes a responsibility to protect both students and the school from abuse of the system.

This policy covers all computers and electronic devices within the school, irrespective of who is the owner. It provides advice and assistance both for boys and parents in the acceptable use of technology at school. In addition to explaining the safe use of email and the Internet, it aims to minimise the chance of cyber-bullying and child exploitation by detailing the only items of mobile technology permissible at school.

Please read this policy carefully – it is important that you fully understand the reasons behind these rules. Only once it has been signed and returned will access to the Internet be permitted. If any boy violates these provisions, access to the Internet will be denied and the boy will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour.

UNACCOMPANIED TRAVEL OVERSEAS:

If any boy has to travel overseas unaccompanied at Long Leave, Short Leave or at the end of term, then if felt appropriate, he may travel with a telephone, subject to the following conditions:

 Other than when traveling, that device must be held in the safe custody of his Lodge Parents.

 The device's charger must be an original product manufactured by the telephone manufacturer.

 The device must be fully insured by the boy's parents.

 Any other items of technology are unwelcome at the school and should be cared for by the boy's Guardian.

Any boy found in possession of an inappropriate item of technology will have that device confiscated and returned to his parents at the earliest convenience. If in addition, the device has been used in an inappropriate manner (bullying, harassing, intimidating, accessing inappropriate material, creating a "mobile hot-spot) the boy would also be subject to the appropriate discipline code.

In summary, devices capable of recording images, video, sound or data; connecting to another device or the Internet wirelessly or via a cable; creating a "mobile hot-spot"; playing games; storing data, video or images; being used for any form of communication, or supporting mobile payment, may not be used by any boy, nor be in the possession of any boy within the school premises or while on school trips.

ACCEPTABLE USE

The purpose of ICT at Summer Fields is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

The use of computers within the School is singularly for the purpose of academic studies.

Boys may not use any classroom computer.

Internet access and email are entitlements for boys who show a responsible and mature approach to its use. The school has a duty to provide boys with quality Internet access as part of their learning experience. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the boys. Boys will be taught acceptable Internet use, and will be given clear objectives for its usage.

All public computers within the school are monitored remotely by e-Safe Forensic Monitoring Service which reports on inappropriate usage. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for boys. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

1. PERSONAL & ONLINE SAFETY

a) When using the Internet, particularly when using social media sites like Facebook, always be extremely cautious about revealing personal details. Never reveal your home address, telephone number, email address, where you are planning to go, the name of your school or photographs of you to strangers.

b) Once you upload photographs, you no longer have control of who sees them. Therefore, only upload photos that you would be happy to show your parents, your future school or your future employer.

c) Ensure that your privacy settings are set to 'private' so that only your 'friends' can see information about you on social media sites.

d) Do not arrange to meet with anyone you have met on the Internet – people are not always who they say they are.

e) If you are being cyberbullied, save any abusive texts, emails or other evidence. Do not respond to the bully. Tell an adult you trust about the problem (your Tutor, your Lodge Parents, the Head of I.C.T., etc.).

f) Visit www.thinkyouknow.co.uk for more information and advice on how to protect yourself online.

g) Always inform the Head of I.C.T. if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.

h) Always be yourself and do not pretend to be anyone (or anything) that you are not while using the Internet.

i) The Internet can become addictive. If you feel you are spending too long on it, please ask a member of staff for advice about whether it is safe.

j) If in doubt, ask a member of staff.

2. SYSTEM SECURITY

a) Access to ICT resources at Summer Fields may only be provided by the System Administrators. A person who has been given such access does not have the authority to extend that privilege to anyone else.

b) Do not attempt to go beyond your authorised access. This includes attempting to log on as another person; sending email whilst masquerading as another person; accessing another person's files; attempting to circumvent security of any host, network or account, etc. Use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

c) Do not give out your password to any other boy – if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password, then change

it immediately. This password should be changed at least once a term and be at least 8 characters long, containing at least one capital letter and number.

d) Do not make deliberate attempts to disrupt the computer system or destroy data.

e) Do not probe, scan or test the vulnerability of the school network or other networks.

f) Do not interfere with; move; nor alter the set-up of any computer or peripheral within the School.

g) Do not consume food or drink within the I.C.T. Suite or while using any computer in the School.

h) Do not use external storage media in the school network (DVDs, memory cards/sticks etc.).

i) Do not play nor attempt to play any games on any computer within the School unless told by a Member of Staff that the game is of educational benefit (e.g. www.ordnancesurvey.co.uk/mapzone/).

j) Do not knowingly break or misuse headphones or other external devices (e.g. mouse, keyboard, scanner, card reader).

k) Your computer account, screen and keystroke action can be remotely monitored by Staff at any time. Every detail of your Internet access is recorded remotely and frequently analysed.

h) Bullying of another person by email or online will be treated with the highest severity.

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

j) If you mistakenly access such material please inform the Head of I.C.T. immediately or you will be held responsible.

k) If you are planning any activity which might risk breaking this policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff of the relevant subject and the Head of I.C.T. must be informed beforehand.

l) Do not attempt to use proxy sites on the Internet.

m) Access to social networking sites (Facebook; Twitter; Instagram; VK,) is blocked and prohibited.

n) Access to Internet chat-rooms is blocked and prohibited.

4. EMAIL & ONLINE COMMUNICATIONS

a) Access in school to external personal email accounts is blocked and prohibited.

b) All email (sent or received) will be content filtered.

c) It is not possible to email other boys within the school.

d) Boys should neither send nor receive email attachments unless work-orientated.

e) You should check your school email once a day for new messages.

f) Do not reply to spam mails as this will result in more spam. Delete them and inform ICT.

g) All emails sent outside the school reflect on Summer Fields so please maintain the highest standards.

h) Do not use email during lessons unless your teacher has given you permission.

i) Do not send or forward annoying or unnecessary messages to a large number of people e.g. spam or chain mail.

j) Do not join mailing lists.

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

l) Email sent to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.

m) Excessive social email use can interfere with learning and may be restricted. It may also be considered harassment under the Protection from Harassment Act 1997.

5. PLAGIARISM AND COPYRIGHT

a) You must acknowledge the source of information used and respect copyright when using Internet material.

b) 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.

c) Respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner.

d) You should be aware of the legal implications relating to the copying and distribution of digital information (CD; DVD; MP3; MP4; DivX etc.). You may neither distribute nor share such files using any aspect of the school network.

6. PRIVACY

a) All files and emails on the system are the property of the school. As such, system administrators have the right to access them if required.

b) Do not assume any email sent on the Internet is secure.

c) Your emails may be inspected at any time without notice.

d) Your computer account, screen and keystroke action can be remotely monitored at any time. All network access, web browsing and mail on the school system are logged and routinely monitored to ensure that this policy has not been broken. If you are suspected of breaking this policy, your account and/or mobile device will be searched by ICT staff.

e) The school reserves the right to search the Internet for inappropriate material posted by boys and to act upon it.

7. SOFTWARE

a) Do not attempt to load any software onto any School computer.

b) Do not attempt to download programs from the Internet onto school computers.

8. SANCTIONS

Failure to comply with this policy may result in action being taken against you, including:

a) A temporary or permanent restriction of Internet access and email use (as appropriate) and/or banning from access to the school computers.

b) An inspection of the user account.

c) Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

d) When applicable, the School may be under an obligation to involve police or local authorities.

9. GENERAL AND BEST PRACTICE

a) The ICT Suite should never contain more than twenty boys and may only be used for work.

b) There is a limit as to the amount of printing you can do. Think before you print – printing is expensive and consumes resources, which is bad for the environment.

c) If someone makes you an offer on the web or via mail, which seems too good to be true, it probably is.

d) Passwords should be alpha numeric i.e. contain both letters and numbers.

e) Observe health and safety guidelines – look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted appropriately. (See the Health & Safety in the Computer Workplace document).

f) Be considerate and polite to other users.

g) House-keep your email regularly by deleting old mail and emptying the Deleted Items folder.

h) Your only involvement with the printers will be to collect work from them. Do not attempt to reload them with paper; turn them on or off; alter their settings; nor drag paper from them.

i) Do not play with nor remove any cables etc. that are attached to a school computer or peripheral.

j) Always log off when you have finished using your computer and leave the surrounding area clean and tidy.

k) If you are leaving the school for good, please ensure you have arranged for any files (or emails you want to keep) to be transferred to memory stick, as these file will be deleted after four weeks.

LEGISLATION

Extensive legislation has been passed to protect technology users from harmful content or actions. The following summarises the Acts of Parliament in place to protect us:

Computer Misuse Act 1990 makes it an offence to erase or amend data or programs without authority; obtain unauthorised access to a computer; "eavesdrop" on a computer; make unauthorised use of computer time or facilities; maliciously corrupt or erase data or programs, and deny access to authorised users. This act has been amended by the Police and Justice Act 2006 and by the Serious Crime Act 2015 – this introduced:

unauthorised acts causing, or creating risk of, serious damage; and making, supplying or obtaining articles for use in offence.

Communications Act 2003 makes it an offence to send by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988 makes it an offence to send an indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety.

Obscene Publications Act 1959 and 1964 makes it an offence to "publish" an obscene article (which can include written material, photographs or films). Publishing includes circulating, showing or electronic transmission of the article.

Protection from Harassment Act 1997 creates both civil and criminal offences of harassment. Harassment is defined as a course of conduct which causes alarm or distress. This means that there must be repeated incidents (more than twice). It is also an offence to cause another person to fear, on at least two occasions, that violence will be used against them.

Protection of Children Act 1978 makes it an offence to take an indecent photograph (or film) of a child. A "child" is anyone under 18 although there are differences involving children over

16 in a marital (or similar) relationship. The definition of "photograph" includes images on a mobile phone, handheld device or stored on a computer and also includes "pseudo-photographs" where images have been manipulated. It is also an offence for someone to distribute or show such images or to have them in his possession with the intention of showing them to himself or others.

Public Order Act 1986 makes it an offence to use threatening, abusive or insulting words, behaviour and images with the intention to cause harassment, alarm or distress. This can apply where a mobile telephone (or similar) is used as a camera or video.

Racial and Religious Hatred Act 2006 makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material, which is threatening.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011 extended the powers in the 2006 Act to give permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.