Earlscliffe (Sussex Summer Schools Ltd)

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Guidelines for Staff and Students

All staff can access the academic network from any school workstation or laptop. Access to the iSAMS system is possible through any device that can access the internet. Access is via codes issued by the School Manager. The school operates its own e-mail server, and all users have an e-mail address (username@earlscliffe.co.uk).

Staff have additional access rights on the system. It is therefore important that passwords are not given to anyone else and that computers are not left logged on.

Fast broadband internet access is available from 7.30 am to 00.00 pm for students and 24hrs a day for staff, and all internet content is filtered. All Internet use and e-mails are monitored and logged. If a website which is blocked is needed for a legitimate reason, for example, a lesson, the external IT network consultant can temporarily disable the filtering for the website if advised in advance. Primarily, the provision of internet access in school is to facilitate lesson preparation and administrative tasks and should not be used for recreational purposes.

At times it may be necessary, for technical reasons, to shut down the system, or part of the system, during the school day. Staff and pupils will be notified accordingly and in due time. Encrypted USB drives can be used to transfer documents for work purposes between home and school. Data storage for individual user accounts is limited and may be rationed. Users will receive a warning if they are likely to exceed the data storage limit. Users are asked, in particular, to delete files that are no longer required from their own area and from shared areas. Virus protection software continuously monitors the network, and staff transferring files between school and home are strongly advised to have up-to-date virus protection at home.

Software installed on the system must be appropriately licensed for the number of machines on which it will be used. The external network consultant will carry out all installations where the software is suitable for the system. Staff must not attempt to install any programs themselves and must respect the licensing laws.

Staff are asked to respect the *Computer Acceptable Use Policy* when using computers on the school's network and to ensure that their classes do likewise.

All classrooms have a fixed data projector and access to a computer.

All computer faults and issues should be reported to the School Manager or direct to the schools outsourced IT providers.

All printing should be of a reasonable amount and should not include unnecessary colour prints.

Computer Acceptable Use Policy

The use of technology is actively encouraged, and with this comes a responsibility to protect both pupils and the school from abuse of the system.

All pupils, therefore, should adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school, irrespective of who is the owner.
All pupils are expected to be responsible on the school wifi network, as they would in classrooms and in other areas of the school. The network is monitored and any inappropriate use will be investigated.

Personal Safety
Always be extremely cautious about revealing personal details and never reveal a home address, phone number or e-mail address to strangers. You should not send anyone your credit card or bank details without checking with a teacher.

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.

You should not play with or remove any cables etc that are attached to a school computer.

Always be yourself and do not pretend to be anyone or anything that you are not on the internet.

You should not arrange to meet with anyone you have met on the internet - people are not always who they say they are. If in doubt ask a teacher or another member of staff.

Prevent Duty – Online Safety
Earlscliffe takes seriously its Prevent Duty. As part of this the School employs (Managed by Red Dragon IT Ltd) filtering /firewall systems to prevent staff, students and visitors from accessing extremist websites and materials. These restrictions are in place both when using school computers and anybody using a personal device via wi-fi.
The School Manager is alerted to any serious and/or repeated breaches or attempted breaches of this policy.

System Security
You should not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mail whilst masquerading as another person, or accessing another person's files. You are only permitted to log on as yourself.

You should not give out your password to any other pupil - 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, change it immediately.

You should not make deliberate attempts to disrupt the computer system or destroy data; e.g. but knowingly spreading a computer virus.

You should not alter school hardware in anyway.

You should not knowingly break or misuse headphones or any other external devices for example printers or mice.

You should not attempt to connect to another pupil's laptop or device while at school. Establishment of your own computer network is not allowed.

You should not eat or drink whilst using a computer outside your room.

You should not e-mail or play games on school computers unless a member of staff has given permission.

Inappropriate Behaviour

Inappropriate behaviour relates to any electronic communication whether e-mail, blogging (for example, online diaries), texting, journal entries or any other type of posting / uploading to the internet.

You should not use indecent, obscene, offensive or threatening language.

You should not post or send information that could cause damage or disruption.

You should not engage in personal, prejudicial or discriminatory attacks.

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

You should not knowingly or recklessly send or post false defamatory or malicious information about a person.

You should not post or send private information about another person without them agreeing first.

You should not use the internet for gambling.

Bullying of another person whether by e-mail, online or via texts, will be treated in the same way as any other form of bullying.

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

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

If you are planning any activity that might risk breaking the *Computer Acceptable Use Policy* (for example, research into drugs for a legitimate project), an appropriate member of staff of the relevant subject must be informed beforehand.

You should not attempt to use anonymous proxy sites on the internet.

You should not take a photo of another student or member of staff without their permission.

E-mail

You should not reply to spam mails as this will result in more spam.

You should not open an attachment from an unknown sender. Inform a teacher as it might contain a virus.

All e-mails sent outside the school reflect on the school so please maintain the highest standards.

You should not send by e-mail any files above 5MB. If in doubt please ask a teacher.

You should not send or forward annoying or unnecessary messages to a large number of people, for example, spam or chain mail.

All inbound e-mail messages are intercepted for ‘spam’ detection. All outbound e-mail messages are intercepted and an appropriate e-mail disclaimer is added to the end of the message.

Plagiarism and Copyright

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

You should 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. This includes music files and the copying of CDs etc.

Privacy

All files and e-mail on the system are the property of the school. As such, System Administrators have the right to access them if required.

You should not assume any e-mail sent on the internet is secure.

All internet browsing on the school system is logged and routinely monitored to ensure the *Computer Acceptable Use Policy* has not been broken. Background monitoring notifies System Administrators to any inappropriate internet activity. At any point System Administrators can see what is happening without the pupil's knowledge.

Monitored internet data can be potentially be disclosed to members of the college's SMT and parents.

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

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

Software

You should not install any software on the school system.

You should not attempt to download programs from the internet onto school computers.
You should not knowingly install spyware or any sort of hacking software or device.

General and Best Practice

Think before you print. Printing is expensive and consumes resources, which is bad for the environment. Priority must be given to pupils wishing to use the computers for school use.

Always log off your computer when you have finished using it.

Always back up your work if you are not saving it on the school system. Work saved on the school system is backed up every night for you, but be careful if you have a copy of your work only on a memory stick as you could lose it.

Storage space on the school network is only for school work; do not store your personal photographs or music files on the school system

Avoid saving or printing huge files (for example, above 15 MB) - if in doubt ask a teacher.

Housekeep your files and your e-mail regularly by deleting old items or unneeded items.

Leave your computer and the surrounding area clean and tidy.

If a webpage for which you that feel you have a legitimate use is blocked, please speak with a teacher. The web page can be unblocked if approval is given.

The internet can be addictive. If you feel you are spending too long on it, please ask a teacher or another member of staff for advice about whether usage is safe.

When leaving school, please ensure that you have saved any files or e-mail which you want to keep to a memory stick or a CD to take home, as these files will otherwise be deleted.

The school's internet connection should be used with consideration for others. Any users found to be using bandwidth inappropriately or unfairly will be excluded from the network.

Other Electronic Devices

The ICT policy above also covers other electronic devices such as laptops, PDAs and mobile phones while they are being used at school. None of these devices, however, is covered by the school's insurance and the school accepts no liability for them. All devices should be PAT tested, security marked and brought to school only if essential. This also includes items such as digital cameras and personal DVD players etc.

Personal Laptops

Boarders may use their own personal laptops, and these can be connected to the college's wi-fi network. Parents should be aware that if they provide alternative internet access, then the school cannot take responsibility for either costs incurred or content accessed.

Mobile Phones and PDAs

You should not use a mobile phone during a lesson except in an emergency.

You should not take photos or video with a mobile phone during lessons unless the member of staff has given permission.

You should not take photos of people without their permission.

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

Music/Video Players, for example, iPods

The use of such devices is not allowed during lessons unless the teacher has given permission.

Do not connect such a device to the school's network / school computers.

Do not break copyright laws by swapping illegal music/video files.

Computer Acceptable Use Policy

Log on only as yourself, and do not give out your password.

You should not e-mail or play games in lessons unless permission has been given. You should use a mobile phone in a classroom only in an emergency or if given permission by a teacher.

You should not use any other device, for example, laptop, MP3 player, in a lesson unless permission has been given.

You should not attempt to bypass school web filters.

Always be polite and respectful to other users, and leave the computer as you found it.

You should not eat and drink at the computer

You should not alter or play with anything connected to the computer.

You should not give out your personal details online, and you should never arrange to meet a stranger.

Be aware that the school can check your computer files and which web sites you visit at any time

You should not use bad language, bully or try to access inappropriate material online.

Always respect copyright laws and do not plagiarise other people's work.

You should be aware that any breach of this policy will result in appropriate disciplinary action.