Mayfield	Policy Name:	Acceptable Use of ICT Policy - Pupil		
	Owner:	Deputy Head		
	Date Approved: By Compliance Committee	8 Nov 2016	Date Approved: by Governance Committee	17 Nov 2016

Introduction

The use of the latest technology is actively encouraged at Mayfield School, recognising its significant benefits. These include not only the ways in which it can support and enhance learning, but also its potential for effective communication and preparation for the world beyond school. The school also has a responsibility to protect students, staff and the School from abuse of the system, and to promote effective and safe use of these technologies

All pupils, therefore, must adhere to the Policy set out below. This Policy covers all workstations, laptops, mobile telephones and electronic devices within the School, irrespective of who is the owner.

All pupils are expected to behave responsibly on the School computer network, as they would in classrooms and in other areas of the School. The use of the School network, computing facilities and the use of girl's own devices in School are privileges, and there may at time be reasonable restrictions made on usage, and sanctions imposed for misuse, as outlined in this policy.

The boarding houses have guidelines for usage after the end of the academic school day and at weekends, which are appropriate to the age group of the girl's resident in the houses, which are outlined in the House handbooks.

Electronic Devices

The policy also covers other electronic devices such as laptops, tablets, mobile telephones, iPods and any other web enabled device, while they are being used at School. However, none of these devices is covered by the School's insurance and the School accepts no liability for them.

All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and mp3 players, etc.

All parents must complete and sign the Electronic Device registration form for any devices that their daughter wishes to bring into School.

The School system has excellent security filters and allows appropriate monitoring. **Parents are advised that if pupils have 3G/4G enabled devices they can bypass our security and filters, and therefore they should be setting up parental controls via their provider. (Each individual provider can give advice on the controls available via their systems).**

Education

Blocking and barring websites and applications is not in itself an adequate method of protecting pupils, especially given the prevalence of easily accessible mobile internet. The school is committed to educating our pupils to understand responsible, safe and effective use of IT, including internet, e-mail and social network use. This takes place within the IT curriculum, the Life Skills programme and the tutor programme.

Use of the Network

All users of the School network are allocated network file space to store school work and materials to support work. Users will also have access to certain shared files, networked printers and other resources as well as e-mail. Once a pupil has left the School, the content of their network files will be deleted.

Use of the Internet and e-mail

These communications facilities are provided as essential teaching and learning tools and we encourage all members of the school community to use them effectively and appropriately. All incoming and out-going electronic data will be monitored for inappropriate content and threats such as computer viruses.

Use of Wireless

The School provides Wireless internet to the academic areas of the school and to boarding houses, and this enables pupils to connect to the internet via Wi-Fi enabled devices. See guidelines on the J Drive, Student Shared S Drive, Systems Support notes, BYOD connections – (Bring Your Own Devices).

Cyberbullying

Bullying in any form is not tolerated at Mayfield School and any incidents will be treated as a serious pastoral and disciplinary issue. Please see the Anti-Bullying Policy for more detail on the School's processes and procedures to prevent and respond to incidents of bullying. Further specific guidance for pupils is found in Section 3 'Inappropriate Behaviour' below.

Sanctions

- Sanctions will vary depending on the severity of the offence; this can range from use of the School's referral and detention system, to suspension or expulsion, as outlined in the school's Rewards and Sanction Policy.

- Specific sanctions such as the withdrawal of network usage and use of electronic devices may also be applied where infractions of this policy have taken place, in line with the framework.

- A breach of the law may lead to the involvement of the police.

  The following sections outline appropriate use of ICT in school and are reviewed regularly with pupils in ICT lessons

1. Personal Safety

- Remember: you are responsible for your actions and conduct on the network and internet, as you are in school life generally.
  Always be extremely cautious about revealing personal details and never reveal a home address, telephone number or email address to strangers
- Do not send anyone your credit card details or any one else's or any other details without checking with an adult first.

- Always inform your teacher or another adult if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.

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

- Do not arrange to meet anyone you have met on the Internet; people are not always who they say they are.
- Do not play with or remove any cables that are attached to a School computer.

- If in doubt, ask a teacher or another member of staff.

2. Extremism and Radicalisation

Some extremist groups who advocate violence use the internet as a means of radicalisation, inciting violence and promoting methods of terrorism. Accessing websites containing such material would be a breach of this policy.

These groups pose a threat both to individuals and to society in general and it is everyone's responsibility to report concerns. If you come into contact with any such material or communication online or are aware that anyone else is accessing such material you must report it, as you would any Safeguarding concern, to the School's Child Protection Officer, who is the Deputy Head. If you have accessed material in error or have been contacted by any such group reporting this immediately enables the School to act in protection of you and the community.

3. System Security

- Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff or as an IT Engineer is unacceptable and may result in the loss of access to systems and other serious sanctions. You are only permitted to log on as yourself.

- Do 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.

- Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters. They must be at least fourteen characters in length and contain characters from three of the following categories:
  Roman uppercase characters (a-z)
  Roman lowercase characters (a-z)
  Numeric characters (0-9)

- Do not make deliberate attempts to disrupt the computer system or destroy data, eg by knowingly spreading a computer virus.

- Do not alter School hardware in any way.

- Memory sticks can only be used on computers that have USB ports.

- Do not attempt to connect to another pupil's laptop or device while at School. Establishment of your own computer network is not allowed.

4. Inappropriate Behaviour

'Inappropriate Behaviour' relates to any electronic communication whether email, blogging, tweeting, social networking, texting, journal entries or any other type of posting/uploading to the Internet.

- Do not use indecent, obscene, offensive or threatening language.
- Do not post or send information that could cause damage or disruption.
- Do not engage in personal, prejudicial or discriminatory attacks.
- Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person.
- Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.
- Do not post or send private information about another person without their prior agreement.
- Do not use the Internet for gambling.
- Bullying of another person either by email, online or via texts will be treated with the highest severity.
- Do 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 may be held responsible.
- If you are planning any activity which might risk breaking the Student Acceptable Use Policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff must be informed beforehand.
- Do not attempt to use proxy sites on the Internet.
- Do not take or post a photo of another pupil or member of staff without their permission.

5. Email

- You should check your School email at least once a day during term time for new messages. It is recommended that those girls using laptops, tablets and smart-phones have access to school e-mail set up on these devices.
- Do not reply to spam mails as this will result in more spam. Delete them and inform the IT Department.
- Do not open an attachment from an unknown source. Inform IT as it might contain a virus.
- All emails sent from the School reflect on the School name so please maintain the highest standards.
- Do not use email (including web mail) during lessons unless your teacher has given permission.
- Do not send any files above 10mb by mail. Please ask IT if you require this temporarily to be lifted.

- Do not send or forward annoying or unnecessary messages to a large number of people, eg spam or chainmail.

- Do not join mailing lists without the prior permission of IT.

- Only send mail to a distribution list if you really have to.

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

6. Plagiarism and Copyright

- 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.

- You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work. You should request permission from the copyright owner. This includes music files and the copying of CDs, downloading of films from illegal sites and other such formats.

7. Privacy

- All files and emails on the system are the property of the School. As such, system administrators and staff have the right to access them if required.

- Do not assume that any email sent on the Internet is secure.

- All network access, web browsing and mails on the School system are logged.

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

- The School reserves the right to randomly search the Internet for inappropriate material posted by pupils and to act upon it.

8. Software

- Do not install any software on the School system.

- Do not attempt to download programs from the Internet onto School computers.

- Do not knowingly install spyware or any sort of hacking software or device.

9. 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. Do not lock the computer so that others cannot use 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 only have a copy of your work on a memory stick or disk as you could lose it.

- Avoid saving or printing sizeable files (eg. above 5mb); if in doubt ask a member of IT.

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

- 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 to the correct height to the desk.

- Be considerate and polite to other users.

- Do not eat or drink whilst using the computer.

- Do not play games by or near any computer equipment

- Housekeep your email regularly by deleting old mail.

- Leave your computer and the surrounding area clean and tidy.

- Do not knowingly break or misuse headphones or any other external devices, e.g. printer or mouse.

- You may use your own headphones only if there is a headphone socket on the front of the workstation.

- If a web page is blocked that you feel you have a legitimate use for, please ask IT and it can instantly be unblocked if approval is given.

- 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.

- If you are leaving the School, please ensure you have saved any files or email you wish to keep to a memory stick or CD to take home, as these files will be deleted.

- If in doubt, ask a member of the IT Department.

10. Mobile Phones

- Do not use a mobile telephone during lessons unless you have the teacher’s permission.

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

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

11. Photographs and Videos

- Do not take photos or videos in school with any device unless the member of staff has given permission.
- Do not take photos of people without their permission.
- Do not post on the internet photographs of school activities without permission.

12. Music/Video Players (e.g. iPods)

- The use of such devices is banned during lessons unless the teacher has given permission.
- Do not connect such a device to the School network/School computers.
- Do not break copyright laws by swapping illegal music/video files.
- Do not listen to music in lessons unless the teacher has given permission.

A copy of this policy is available on the School website: www.mayfieldgirls.org.

Mayfield

Pupil Acceptable Use of ICT Policy

Pupil Name: ____

I have read and I understand the School's Pupil Acceptable Use of ICT Policy. I shall use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: ____

Print name: ____

Date: ____

Parent/Guardian:

As a Parent or Guardian I have read this agreement. I understand that although Mayfield School employs the mail defence and web defence technology, no system can be 100% safe. I give my daughter permission to use the School computer system:

Signed: ____

Print name: ____

Date: ____

Appendix 1

The Quick Guide: Pupil Computer, Mobile and iPod Use

- You may only log on as yourself. Do not give your password to anyone else. Always log off at the end of a session of computer use.
- Be aware that the School can check your computer files and which sites you visit at any time.
- Do not use bad language, bully or try to access inappropriate material on line.
- iPods and mobile telephones must be switched off and out of sight during lessons unless permission has been given by the teacher to use them. Mobile phones may be used in Main School during break and lunch but may only be used at break and lunch in Lower School with the permission of the supervising member of staff.
- Internet browsers may not be switched on during lessons unless permission has been given by the teacher to use the internet.
- Under no circumstances are you to use social networking sites, email or Skype during lesson time.
- You are not to record, video or photograph anything during lessons unless the teacher requests that you do so.
- You must not wear earphones when walking around the site at any time.
- Do not attempt to bypass school web filters.
- Do not give out your personal details online and never arrange to meet a stranger.
- Respect copyright and do not plagiarise work.

Any breach of this policy will result in appropriate disciplinary action.

Appendix 2

1. **SMART Rules – to display in form rooms**

S **Safe** - Keep safe by being careful not to give out personal information, such as your full name, email address, telephone number, home address, photos or School name, to people you have only had contact with online. Set strong privacy settings on social networking sites

M **Meeting:** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or guardians' permission and even then only when they can be present.

A **Accepting:** Accepting emails, instant messages, or opening files, pictures or texts from people you don't know or trust can lead to problems; they may contain viruses or nasty messages!

R **Reliable:** Information you find on the Internet may not be true, or someone online may be lying about who they are.

T **Tell:** Tell your parents, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at: www.thinkyouknow.co.uk and you can report anything you are not happy about to anyone you feel you trust. This could be a teacher, guardian, parent or someone else's parent. Tell someone.