Emerson Park Academy

A SPECIALIST SPORTS COLLEGE

ENDEAVOUR
PERSEVERE
ACHIEVE

# ACCEPTABLE USE POLICY for PUPILS

**Updated: January 2016**

**'Acceptable and Responsible Use of ICT Resources'**

## Contents

## 1 THE BENEFITS OF INTERNET ACCESS FOR EDUCATION

Most curricula at European level require pupils to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the Internet offers both pupils and teachers vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between pupils from all over the world, while at the same time providing access to educational, social and leisure resources. The increased use of the Internet in the classroom has totally revolutionised the way that research is carried out in school. In just a few keystrokes it is possible to obtain tons and tons of information from a variety of online resources from a diverse range of organisations or individuals on a global scale.

The main reason that we provide Internet access to our teachers and pupils is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both pupils and teachers, Internet access at school is a privilege and not an entitlement. Unfortunately as there is the possibility that pupils will encounter inappropriate material on the Internet, the school will actively take all reasonable precautions to restrict pupil access to both undesirable and illegal material. The school makes extensive use of managed filtering systems and regularly audits internet logs to ensure that all users access on-line resources in a responsible manner.

Within the classroom, teachers are responsible for guiding pupils in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that pupils are only too aware of what is regarded as acceptable and responsible use of the Internet. The main goal is to utilise Internet access to enrich and extend those learning activities that reflect the curriculum requirements and the age and maturity of the pupils.

Pupils will access websites from bookmarks within the ‘Favourites’ folder in their browser. These will have been previewed and approved by their teacher. All Internet access is filtered through a proxy server to screen out undesirable sites at source. All users have a responsibility to be vigilant and careful whenever they engage in on-line activities. Users should be cautious when using keywords or phrases in search engines as the results can often return matches to undesirable and/or unrelated material.

Whilst the Internet does a lot for pupils and teachers, there are also numerous benefits for parents. The interactive learning that the Internet provides can help pupils and parents with minimal command or no English skills to learn the English language. This enables parents to become more involved in their children's education by connecting the school with homes, libraries or other access ports.

Teachers can adjust to the different learning styles and in the classroom. They can also set their own pace of teaching. Individual teaching techniques can become more available, which has been proven to be a factor in pupil achievement.
The Internet and its connective technologies, enables teachers to be able to teach to larger audiences in more than one place simultaneously. They may be in a small town but through the Internet, they can be linked to pupils in more populated areas.

## 2 WHOLE-SCHOOL NETWORK SECURITY STRATEGIES

The school’s computer network security systems are reviewed regularly at the end of each term by the ICT Technical Support team and Head of BCI Faculty. Any recommendations for change or concerns are reported to the Head Teacher so that appropriate procedures can be administered to safe-guard the integrity of network resources and data.

The school will regularly check user files, temporary Internet files and history files to monitor appropriate and responsible usage and take appropriate action if a violation to the school's AUP is discovered.

Uploading and downloading of non-approved application software is denied as this could contravene copyright regulations.

All access to the school network requires entry of a recognised User ID and password. Pupils must log out after every network session or whenever they expect to be away from their workstation for more than a few minutes. This will minimise problems such as a breach of trust or unauthorised use of another user's network account. Pupils who do not log out at the end of sessions or leave their workstations unattended, could have their access to network resources restricted or suspended for a set period of time.

Anti-Virus protection software is installed on the network and updated regularly to minimise the threat of data contamination and security breech. Users are encouraged to report any suspicious files or unusual application behaviour to the ICT Technical Support team or their ICT/Computer Science teacher for further investigation.

The use of external hard drives, DVD / CD-ROMs or USB flash drives (Memory Sticks) on the school network is not advised as they have associated security risks. Viruses could be easily transferred from a home computer system to the school network if anti-virus protection is not installed on an external computer system or is not up to date. As a consequence, users must seek permission from the ICT Technical Support team or their ICT/Computer Science teacher for use of storage media in conjunction with network resources. Specific instructions and training for virus checking will be provided in KS3 Computer Science lessons.

Alternative file storage is available for transferring files from school to home via Google Drive. Users may be able to access other forms of cloud storage with the permission from the ICT Technical Support team. Specific instructions and training for data transfer is provided in KS3 Computer Science lessons.

Unapproved system utilities software and executable files are not allowed to be stored in pupil storage areas.

Pupil files held on the school's network are monitored on a regular basis by the ICT Technical Support team. Pupils are advised to organise their user area so that data management can be optimised and redundant data is removed in order to preserve the operating capacity and performance of the network.

### Networks Essentials

Network accounts are to be used only by the authorised owner of the account.

If a user finds a computer logged in and is unattended, they should do nothing in that account except for logging the current user off the network providing they have the permission from supervising staff.

It is the responsibility of pupils to make backup copies of their work and training will be provided in KS3 Computer Science lessons. The school will exercise due care with backups and regularly test backups in order to minimise any incident of lost data.

Pupils must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Pupils are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause school rules to be broken.
- Use or possess any program designed to reduce or compromise network security
- Enter any other user's home directory or do anything whatsoever to any other person's files
- Use another user's email account
- Access the Internet using another user's account unless they are working in groups and have the permission from staff and the account owner
- Attempt to alter any user's access rights
- Store the following types of files in their home directory, without permission from the ICT Technical Support team:

    - Program files (EXE, COM, BAT)
    - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)

- Store unnecessary image/video/audio files, unless they are required by a subject
- Access or create obscene material – images, video, audio or text
- Use obscene filenames
- Access or create insulting or offensive material
- Create unnecessary password-protected files that are required for examination purposes
- Store or distribute copyrighted material – images, video, audio or text
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

## Hardware and software infrastructures

The school has invested in the following hardware and software infrastructures to reduce risks associated with the Internet:

- Proxy server – in conjunction with a web management system
- Client Server network – in conjunction with an information and web management system
- Filtering software
- Walled garden
- Firewall – that has been configured to prevent access to inappropriate websites.

### Virtual Networking and Remote Access

Pupils accessing school resources via the virtual network are subject to the same rules that apply to the main school computer network.

Pupils must use their virtual network account in accordance to the Pupil's AUP.

Pupils are only permitted to use the resources installed by the ICT Technical Support team and must not install program updates, their own applications or download resources without permission from the ICT Technical Support team.

### Classroom management structures

Planned seating will allow teachers to trace and monitor pupil access and usage of the Internet. All staff are required to complete a seating plan for classes using the main ICT rooms and pass the details to either the ICT Technical Support team or Head of BCI Faculty for the purpose of auditing and monitoring.

The main ICT rooms are equipped with specialist network management software called 'NetSupport ', which enables computers to be controlled and monitored by both the classroom teacher and remotely by the ICT Technical Support team. Training is available by arrangement with the Head of BCI Faculty.

## 3 RISK ASSESSMENT AND MANAGEMENT OF INTERNET CONTENT

The school has taken and will continue to take all reasonable precautions to ensure that pupils access appropriate material only. However, it is not possible to guarantee that a pupil will never come across unsuitable material while using a school networked computer. The school, however, cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

All pupils are taught effective online research techniques, including the use of subject catalogues and search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received;
- Using alternative sources of information for comparison purposes;
- Identifying an author's name, date of revision of the materials, and possible other links to the site;
- Respecting copyright and intellectual property rights.

Throughout their schooling, pupils will receive e-safety guidance in KS3 Computer Science lessons and through Year Group assemblies each year. It is important to provide pupils with key information and reminders of acceptable computer usage in order to safe-guard them from danger and to ensure that they conduct themselves as responsible digital citizens.

Pupils will be made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, extremism, racism and exploitation of children.

However, if they encounter such material they will know that they should switch off the monitor, not the computer, and report the incident to the nearest teacher and to a member of the school's E-Safety Committee who will deal with it according to the school AUP.

## 4 REGULATION AND GUIDELINES

The school's Internet access incorporates a software filtering system to block certain chat rooms, newsgroups, and inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate sites is blocked.
- Access will be allowed only to a listed range of approved sites.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- A rating system is used to rate web pages for inappropriate content and that the web browsers are set to reject these pages.
- Records of banned Internet sites visited by pupils and teachers are logged.

Accessing a site denied by the filtering system will result in a report being generated and passed onto the Head of BCI Faculty for appropriate action.

The Head of BCI Faculty and the ICT Technical Support team regularly assess the effectiveness of the filtering system. The school's filtering strategy depends on the age and curriculum requirements of each class. Staff are advised to check links to external sources as the filtering system can prevent access to a valid and appropriate source. The ICT Technical Support team will check links blocked by the filtering system and may add them to a 'safe' or 'exception' list so that access is possible in lessons.

### 4.1 E-mail accounts

Pupils may only use their approved e-mail account/s (currently GMAIL) on the school network during school time.

Pupils shall immediately report any offensive e-mails that they receive to their teacher. They will be taught not to delete the evidence and advised not to discuss it with other pupils as this could compromise any investigations.

Access in school to external, Web-based, personal e-mail accounts is denied for network security reasons.

It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender. Pupils will be taught e-mail etiquette and advised how to deal with junk mail so that the school email system does not get cluttered with unnecessary network traffic which will ultimately slow down the network.

Pupils must read their e-mails regularly and remove superfluous e-mails from the server.

Pupils may send spam messages only if they are required to do so as part of, for example, project work. Permission from the teacher will always be required to do this.

Pupils may not reveal their own or other people's personal details, such as addresses or telephone numbers or arrange to meet someone outside school via the school network.

Sending and receiving e-mail attachments is subject to permission from the teacher and pupils must be careful not to open attachments that appear suspicious or are from unknown/anonymous senders.

### 4.2 Network Etiquette and Privacy

Pupils are expected to abide by the generally accepted rules of network etiquette.

These rules include, but are not limited to the following:

***BE POLITE.*** Never send or encourage others to send abusive messages.

***USE APPROPRIATE LANGUAGE.*** Remember that you are a representative of the Academy on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

***PRIVACY.*** Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other pupils.

***PASSWORD***. Do not reveal your password to anyone. If you think someone has obtained your password, report this to a member of ICT Technical Support team immediately.

***ELECTRONIC MAIL***. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.

***DISRUPTIONS***. Do not use the network in any way that would disrupt use of the services by others. E.G. Streaming videos or downloading unauthorised media or applications from an external website.

**OTHER CONSIDERATIONS**:

- Be brief but concise in message. Few people will bother to read a long message. Proof read your message to ensure that it is error free and easy to understand.
- Remember that humour and satire are very often misinterpreted.
- Always cite references for any facts or information that you present. Do not copy other people's work and imply that it is your own. If you do so you are almost certainly guilty of plagiarism. Plagiarism at GCSE level will undoubtedly lead to formal action, up to and including, withdrawal from examination and qualifications.
- Respect the rights and beliefs of others.

### 4.3 The school's website

The school webmaster or ICT Technical Support team manages all aspects of placing web pages on the school's website. It has full editorial responsibility and ensures that the content on the site is accurate and appropriate. The website will comply with the Education Authority's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about teachers' home addresses or the like will be published.

The school will not publish any material produced by pupils without the agreed permission of their parents. In addition, photographs of pupils will not be published without a parent or carer's written permission. A pupil's full name will not be used in association with photographs.

Website photographs that include pupils will be carefully selected and will be of a type that doesn't allow individual pupils to be identified - group photographs or 'over the shoulder' images are preferred.

Only regulated educational chat environments shall be used. They will always be used under supervision. Safety is the major consideration.

Only newsgroups that have educational goals and content will be made available to pupils via Google Classroom or a similar collaboration resource.

### 4.3 Moderated mailing lists, newsgroups and chat rooms

The school may use an e-mail distribution list to send messages to selected groups of users.

Teachers will moderate collaboration tools such as newsgroups, blogs and forum rooms in Google Classroom or a similar collaboration resource when used on the school network for learning purposes.

Pupils will be denied access to public or unmoderated chat rooms.

### 4.4 Other communication technologies

Pupils are not allowed to use mobile communication devices during lessons or formal school time unless they have been given permission by their teacher who will closely supervise the activity. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by or accessible through the school network. Similarly, the recording of audio within the school is prohibited unless it has been authorised by a teacher in relation to a project or coursework evidence.

### Integrated cameras

Cameras integrated into mobile phones, tablet computers or laptops can be used in lessons to collect evidence for coursework for example but permission must be given by their teacher. Using the camera or audio functions of the phone or tablet without permission will lead to sanctions according to the school's behaviour policy.

It is not uncommon for pupils to take photographs and video footage and post these to social media or similar websites. Since the taking of unauthorised images is not allowed in school it follows that putting images or uploading video content taken in school is not allowed and will most certainly result in pupils being punished and the incident being dealt with in the appropriate manner.

Sanctions may include not being allowed to bring a mobile phone or mobile communication device to school and/or being excluded from school. Pupils downloading these images or video may also be punished.

### Mobile phone misuse outside school

Mobile phone misuse is not restricted to occurrences in school. It may involve misuse outside of school and can adversely affect other pupils or staff and is taken very seriously.

Examples of misuse include:

- Taking, transferring or storing inappropriate material of others without permission
- Harassment or bullying by phone or text
- Uploading or downloading photographs or video footage taken in school.
- Recording audio created from within school and transferring or sharing it without permission

If mobile phone misuse outside school is found to be affecting pupils or staff in school, the parents/carers of the pupil(s) involved will be contacted and sanctions (e.g. punishment exercise; removal of permission to bring mobile phone to school; exclusion) are likely to be applied.

### Bring Your Own Device (BYOD)

Pupils choosing to connect their personal devices to the Academy's wireless network accept that, where appropriate, they must comply with the requirements and terms of this AUP policy and must realise that the Academy cannot be responsible for damage or theft of devices brought in from home.

## 4.5 Computer Network and Internet/E-mail Protocol

### The following are Breaches of Computer Network and Internet Protocol

1. Using chat, network chat or messenger services on the network or the Internet.

2. Setting up bogus school email accounts or linking school email accounts to unsolicited mail services.

3. Creating online petitions/surveys connected to the Academy without the permission of the appropriate member(s) of staff.

4. Accessing non-schoolwork related material on the internet or sending and receiving such material via school web-mail.

5. Gaining or attempting to gain access to the network, Internet and/or E-mail whilst having access denied for not adhering to the school's AUP.

6. Sending or attempting to send any unsuitable/inappropriate material using the schools network and internet services or personal mobile phones *("Unsuitable" is defined as words/statements/material relating to computer based games (including consoles), material of a sexual nature, obscene/swear words, items relating to non-conformist groups or groups of questionable origin/beliefs/political views.)*

7. Typing an unsuitable/inappropriate key word/s into a search engine and/or typing an unsuitable/inappropriate URL (website address) into the address bar of any web browsing software package.

8. Having, saving or attempting to save any unsuitable/inappropriate and/or malicious material:

   - In your own user area
   - In a shared network area such as Pupil Common Drive
   - In your school Google Drive account or any accessible school virtual network
   - On a laptop/palmtop/notebook/tablet, mobile phone or any other electronic device
   - On a DVD/CD/USB device or any other storage medium in school

9. Viewing or attempting to view or download unsuitable/inappropriate material

10. Entering or attempting to enter a suspect website despite warnings from the Internal Web Filtering Service about unsuitable content.

11. Using another person's network account to access services such as network resources, the internet, email facilities, etc.

12. Using staff designated ICT resources such as the teacher's classroom workstation where access to sensitive data must be restricted unless close supervision is ensured throughout its usage.

13. Damaging or attempting to damage any ICT resources or equipment in school.

14. Moving, interfering with or attempting to repair any ICT equipment without permission from an ICT teacher or member of the ICT Technical Support team.

15. Removing ICT resources from its fixed or normal location without permission from an ICT teacher or member of the ICT Technical Support team.

## 5 COMMUNICATING THE SCHOOL'S AUP

### 5.1 Informing pupils

'Code of Practice' posters will be displayed near all networked computer systems. Pupils will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet. Pupils and Parents must sign the relevant part of the AUP before being allowed network access.

### 5.2 Informing staff

All staff will be provided with a copy of the School's Acceptable Use Policy. Teachers are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted regularly about the development of the school's Acceptable Use Policy and instructions on safe and responsible Internet usage. Teachers will also sign the Acceptable Use Policy for Staff.

To avoid misunderstandings teachers can seek clarification from the Academy's e-Safety Co-ordinator regarding any doubts that arise concerning the legitimacy of any given instance of Internet use. Teachers will be provided with information on 'copyright and the Internet' issues that apply to schools.

### 5.3 Informing parents / carers

Parents' attention will be drawn to the School AUP by letter, in Pupil Planners and on the school's website. Advice that accords with acceptable and responsible Internet use by pupils at home will be made available to parents. Safety issues will be handled sensitively. The school will obtain parental consent before publication of pupils' work or photographs on the Internet

See checklist overleaf:

# *** Checklist for Parent/Carers ***
# Acceptable Use Policy

- I have read and discussed the Acceptable Use Policy (attached) with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with appropriate schools policies. If the school believes that my child has committed a criminal offence then the school may well contact the Police or other appropriate authorities
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately print, upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school e-Safety Coordinator (Mr Galliano), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- I am aware that I can visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I am aware that I can visit external agencies for more information about keeping my child(ren) safe online: www.nspcc.org.uk/onlinesafety, www.thinkuknow.co.uk/parents , www.internetmatters.org , www.childnet.com and www.saferinternet.org.uk
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

**I have read the Pupil Acceptable Use Policy.**

Child's Name………………………………………. Tutor Group…………………………

Parents Name………………………………..... Parents Signature………………………….

Date…………….

http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety