Emerson Park Academy

ACCEPTABLE AND RESPONSIBLE USE OF ICT RESOURCES POLICY FOR PUPILS

Reviewed: March 2023
Next Review: March 2026

'Acceptable and Responsible Use of ICT Resources'

Contents

1 THE BENEFITS OF INTERNET ACCESS FOR EDUCATION

Most curricula at European level require students to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the Internet offers both students and teachers vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between students from all over the world, while at the same time providing access to educational, social and leisure resources.

The main reason that we provide Internet access to our teachers and students is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both students and teachers, Internet access at school is a privilege and not an entitlement.

Unfortunately as there is the possibility that students will encounter inappropriate material on the Internet, the school will actively take all reasonable precautions to restrict student access to both undesirable and illegal material.

Teachers are responsible for guiding students in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that students 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 students.

2 WHOLE-SCHOOL NETWORK SECURITY STRATEGIES

The school's computer network security systems are reviewed regularly at the end of each term by the IT Manager.

Uploading and downloading of non-approved application software is denied.

All access to the school network requires entry of a recognised User ID and password. Students must log out after every network session.

Virus protection software is installed and updated regularly.

Using personal floppy disks, CD-ROMs or USB Memory Sticks on the school network requires specific teacher permission and a virus check.

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

Hardware and software infrastructures

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

- Client Server network – in conjunction with an information and web management system
- Anti-Virus software
- NetSupport – PC monitoring software
- Web Filtering software
- Smoothwall – digital safeguarding solutions
- Firewall – that has been configured to prevent access to inappropriate websites.

Classroom management structures

Planned seating will allow teachers to trace and monitor student access and usage of the Internet.

Ensure that computers are monitored during each lesson by deploying NetSupport software.

3 RISK ASSESSMENT AND MANAGEMENT OF INTERNET CONTENT

The school has taken and will continue to take all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student 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 students 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.

Students 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, 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 or the school's E-Safety Co-ordinator 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 students and teachers are logged.

The school's ICT Manager regularly assesses the effectiveness of the filtering system. The school’s filtering strategy depends on the age and curriculum requirements of each class.

4.1 E-mail accounts

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

Students shall immediately report any offensive e-mails that they receive to their teacher.

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.

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

Students 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.

Students 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.

4.2 The school's website

An editorial 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 students without the agreed permission of their parents. In addition, photographs of students will not be published without a parent or carer's written permission. A student's full name will not be used in association with photographs.

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

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 other collaboration tools such as newsgroups and chat rooms in GAPPS when used on the school network for learning purposes.

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

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 students.

4.4 Other communication technologies

Students are not allowed to use mobile devices during lessons or formal school time. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network.

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

3. 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.

4. 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.)

5. 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.

6. 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
   - On a laptop/palmtop, mobile phone or any other electronic device
   - On a floppy disc/CD/USB device or any other storage medium in school

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

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

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

10. Moving any ICT equipment without permission from a teacher

5 COMMUNICATING THE SCHOOL'S AUP

5.1 Informing students

'Code of Practice' posters will be displayed near all networked computer systems. Students will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet. Students 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 will contact the 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 students at home will be made available to parents. Safety issues will be handled sensitively. The school will obtain parental consent before publication of students' work or photographs on the Internet.