RHOS Y FEDWEN

Rhos y Fedwen Primary School

Pupil “Acceptable Use Policy of ICT Technology”

1. Privileges

The school has provided chrome books, ipads and other ICT equipment/peripherals for use by pupils, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The chrome books, ipads and other ICT affiliated equipment/peripherals are provided and maintained for the benefit of all pupils, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor.

2. Privileges

2.1. The use of the School's Network, Internet Access and ICT affiliated equipment is a privilege, not a right, and inappropriate use is solely determined by the Head teacher. Failure to comply with the outlined "Acceptance Use Policy" will result in revocation of those privileges at any given time. School may deny, revoke, or suspend a student if he/she is found to be abusing the privilege of using the Internet and World Wide Web. A log of all Network and Internet access and activity is monitored continuously by the IT department so misuse of the system can be quickly identified and dealt with.

3. System Access

Pupils will be granted access to the Rhos y Fedwen system as appropriate once the outlined conditions cited in clause (3) 1.1. have been met:-

1.1. Upon receipt of a "signed parent/guardian slip" (attached), which acknowledges the Acceptable Use Policy outlined.

4. Internet Filtering (smoothwall)

4.1. All Internet access will be filtered for pupils and staff on computers with Internet access provided by the school. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet access to inappropriate website(s)/information. Specifically, as required by the Children's Internet Protection Act, the categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling. Users must not use proxy or “anonymous” sites or other measures to circumvent the filtering system.

4.2. Requests from users who wish to use a blocked website for bona fide research or other lawful purposes may be considered. Please see your STEM Lead or Headteacher to submit a request.

5. Equipment

5.1. Always get permission before installing, attempting to install or storing programs of any type on the computers.

5.2. Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.

5.3. Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.

5.4. Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.

5.5. Always check mobile equipment (e.g. laptops, tablet PCs, etc.) with anti-virus software, and ensure they have been found to be clean of viruses, before connecting them to the network.

5.6. Protect the computers from spillages by eating or drinking away from ICT equipment.

6. Security and Privacy

6.1. Protect your work by keeping your password to yourself; never use someone else’s logon name or password.

6.2. Always avoid revealing your home address, telephone number, school name, or picture to people you meet on the Internet.

6.3. Other computer users should be respected and should not be harassed, harmed, offended or insulted.

6.4. To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.

6.5. Computer storage areas and USB pen drives may be reviewed by staff to ensure that you are using the system responsibly.

6.6. Students may not use another individual‘s account without written permission from that individual.

6.7. Students may not access resources for which they do not have expressed permission.

7. Internet

7.1. You should access the Internet only for study or for school authorised/supervised activities.

7.2. Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

7.3. Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by "copyright laws" (Refer to section 6).

7.4. 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' features of any sort are strictly prohibited.

8. E-Mail

8.1. Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

8.2. Only open attachments to e-mails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

8.3. If you receive an e-mail containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a classroom teacher. The sending or receiving of an e-mail containing content likely to be unsuitable for children or schools is strictly forbidden.

8.4. Note that electronic mail (e-mail) is not private. System operators have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

9. Network

9.1. Do not use the network in such a way that you would disrupt the use of the network by other users.

9.2. All communications and information accessible via the network should be assumed to be private property.

9.3. Do not reveal the personal address or phone number of ANY pupil, sibling or colleague.

9.4. All communications and information accessible via the network should be assumed to be private property.

9.5. Do not go looking for security problems, as this may be construed as an illegal attempt to gain unauthorised access to the system(s). If a potential security issue has been identified, you must report the issue immediately to a classroom teacher or ICT network officer(s) immediately.

10. Plagiarism & Copyright Infringement

10.1. Pupils will not plagiarise work(s) that they find on the Internet. Plagiarism is taking the idea(s) or writing(s) of others and presenting them as if they were original to the user infringing the said content.

10.2. Pupils will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work of another, he/she should request permission from the copyright owner in written letter. Upon written authorisation approving the use of their content may your child(ren) then use the work of the copyright holder

11. Quality of Service (QoS)

11.1. The school cannot be held responsible for any loss of data as a result of technical difficulties. The quality and reliability of any information used to complete schoolwork as a result of research using the Internet, must also be checked with a member of staff. All communications and information accessible via the network should be assumed to be private property.

11.2. Rhos y Fedwen Primary School cannot be held responsible for any interruption in service(s) due to unforeseen circumstances, this includes but is no limited too “power outage, short-circuit, hardware fault, software bug or human-error”.

11.3. STEM Lead and SRS staff ensures that all service(s) are maintained on a daily basis to ensure maximum uptime of its service(s).

12. Monitoring & Surveillance

12.1. As with all other school policies and guidelines, all staff share the responsibility of monitoring and guiding pupils in the appropriate use of technology. Failure to follow these guidelines may result in suspension or termination of privileges and other disciplinary action consistent with the Student Code of Conduct and Local authority policy. Violations of law may result in criminal prosecution.

13. Disclaimer

13.1. Rhos y Fedwen Primary School “IT System(s)” is provided on an “as is, as available” basis. The school does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The school does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the pupil’s requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

ICT - abbreviation for “Information and Communications Technology”

IT - abbreviation for “Information Technology”

Internet - a vast computer network linking smaller computer networks worldwide. The Internet includes commercial, educational, governmental, and other networks, all of which use the same set of communications protocols.

Virus - a segment of self-replicating code planted illegally in a computer program, often to damage or shut down a system or network.

Anti-Virus - Programs to detect and remove computer viruses.

E-mail (“Electronic Mail”) - a system for sending messages from one individual to another via telecommunications links between computers or terminals.