West Monmouth School

Ysgol Gorllewin Mynwy

ICT Acceptable Use Policy

Polisi Defnydd Derbyniol TGCh

Date Approved by Governors: .....

Date Reviewed by Governors: .....

1. Internet Access for Education

National Curriculum documents, GCSE and other Level 1 and 2 specifications require students to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the internet offers both learners and staff 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 staff and learners is to provide educational excellence by facilitating resource sharing, innovation and communication. However, for both learners and staff, internet access at school is a privilege and not an entitlement.

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

Teachers are responsible for guiding learners in their on-line activities, by providing clear objectives for internet use. Teaching staff, who should be mindful of their own acceptable use of ICT (page 8), will also ensure that learners 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 learners.

The use of search engines is permitted only when another teacher or member of staff is present. Staff should contact the ICT technician if they think inappropriate sites are accessible.

2. Whole-School Network Security Strategies

The schools' computer network security systems are managed by the LA who liaise with the ICT technician.

Uploading and downloading of non-approved application software is denied and restricting the use of pen drives facilitates this.

All access to the school network requires entry of a recognised User ID and password. Students must log out after every network session or lock computers if they are not using the computer for a period of time in the lesson.

Virus protection software is installed and updated annually by the LA.

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

Audio/visual and flash/gaming files held on the school's network are deleted regularly.

2.1 Hardware and Software Infrastructures

The LA and the school have invested in the following hardware and software infrastructures to reduce risks associated with the internet:

Proxy server
Client server network
Filtering software
Firewall
Browse control used by staff to manage pupil use of ICT

2.2 Classroom Management Structures

Teachers should monitor learner access and usage of the internet during lessons.

3. Risk Assessment and Management of Internet Content

The school has taken and will continue to take all reasonable precautions to ensure that learners 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.

Learners at West Monmouth School are taught (via KS3 ICT lessons) 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

Learners will be made fully aware of the risks to which they may be exposed while on the internet. Staff should structure tasks appropriately to discourage poor use of sources. They will be shown how to recognise and avoid the negative areas of the internet such as pornography, violence, racism and exploitation of children.

E-Safety is currently covered through the PSHE curriculum at Key Stage 3. All pupils receive a PSHE lesson on e-safety ('Thinkuknow' lesson – lesson plan available to download at: http://www.schoolbeat.org) delivered by the School Police Liaison Officer. This lesson is then followed up by lessons delivered by PSHE teachers as part of the 'Safer Relationships' unit of work in Year 9, using some of the resources provided by the police 'All Wales Schools Liaison Core Programme'.

Pupils are also made aware of e-safety through assemblies delivered by the School Police Liaison Officer that focus on this topic.

If learners do encounter material they know to be inappropriate they should switch off the monitor, not the computer, and report the incident to the nearest teacher who will deal with it according to the school AUP.

4. Regulation and Guidelines

The school's internet access incorporates software installed by the LA to block certain chat rooms, newsgroups and inappropriate websites. The filtering system used on the 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.

- Records of banned internet sites visited by learners and teachers should be logged with the ICT technician.

Accessing a site denied by the filtering system will result in a report being generated and sent to the school's ICT Technician for appropriate action. This could result in an individual's internet access being restricted.

The school's ICT Technician, by corresponding with the LA, regularly assesses the effectiveness of the filtering system, collaborating with staff who have identified issues.

Similarly, the school will request of the LA that certain banned sites be made accessible and provide the educational reasons behind the request.

4.1 E-mail Accounts

Learners should use their approved e-mail accounts on the school network during school time, although other accounts may be used if deemed necessary.

Learners shall immediately report any offensive e-mails that they receive to the class teacher.

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

Learners 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

The ICT Technician and Website Co-ordinator manage all aspects of placing web pages on the school's website. They have full editorial responsibility and ensure that the content on the site is accurate and appropriate.

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 addresses, e-mail addresses, fax and telephone number. No information about teachers' home addresses or the like will be published. Names of staff and qualifications are also included.

The school will not publish any material produced by learners without the agreed permission of their parents. In addition, photographs of students will not be published without a parents or carer's written permission.

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 if used on the school network for learning purposes.

Learners 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.

It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network.

5. Communicating the School's AUP

5.1 Informing Learners

'Code of Practice' posters will be displayed near all networked computer systems. Learners will be informed that their internet use is monitored and be given instructions on safe and responsible use of the internet. Learners must sign the relevant AUP, together with their parents/carers, before being allowed network access.

5.2 Informing Staff

All staff will be provided with a copy of the School Acceptable Use Policy. All staff 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 AUP and instructions on safe and responsible use of the internet. Staff will also sign the relevant part of the AUP document.

To avoid misunderstandings, staff will contact the member of the SLT with line manager responsibilities to ICT regarding any doubts that arise concerning the legitimacy of any given instance of internet use.

5.3 Informing parents/carers

Parents' attention will be drawn to the School AUP by the school newsletter and the school brochure and the policy will also be put on the school website. Pupils, parents and carers who do not sign the AUP from two weeks of its distribution will not be able to access the school network. 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.

All comments on and suggestions concerning this Acceptable Use Policy should be sent to:
Andrew Protherough Jones.

WEST MONMOUTH SCHOOL ACCEPTABLE USE AGREEMENT

This AUP helps to protect the school and its learners by describing acceptable and unacceptable computer use.

Access

- I will respect system security and I will not disclose any password or security information to anyone.
- I will not download or install any software or files on schools ICT equipment.
- I will not attempt to bypass any computer or network security settings.
- I will only use the school network for school purposes.

Internet

- I will ensure that any contact through ICT including email and instant messaging to other adults and pupils is responsible, polite and sensible.
- I will not set up any internet accounts in school without permission from a member of staff.
- I will take responsibility for my own e-safety and adhere to the e-safety rules in West Monmouth School. This includes not giving my personal details to people online, unless advised by a member of staff.
- I will never put my school details online including address and phone numbers, unless advised by a member of staff.
- I will only use my school email address for school related purposes.
- I will not open attachments, using my school email address, from any unknown sources.
- I will not attempt to access any unsuitable, inappropriate or illegal websites. If I do this by accident I will report it to my teacher as soon as possible for the safety of others in school.
- I will not invite my teachers or other members of staff to be friends on any social networking site (other than those used for education or school related sites).
- I will not use any applications or services to bring West Monmouth School or any of its members into disrepute.

Storage

- I will only store school related files and images on the school network.
- I will use the LMS to transfer files between home and school.
- I will avoid using a USB pen wherever possible and if I do, make sure it has been anti-virus checked. The device will only be used when permission has been sought from a teacher and approval has been given from the ICT technician.
- I will regularly review my files and delete them when appropriate.

Use of equipment

- I will treat all ICT equipment and devices with care and use only with permission from a teacher or member of staff.
- I will report any damage, viruses or problems to my teacher as soon as possible, who will notify the ICT technician.
- I will not use any school ICT equipment or devices for my own personal use, but only under the direction or guidance of a teacher or member of staff.
- I will only take photographs or video of people with their permission and will only use them for the purposes for which they have given their permission.
- I will turn off my mobile phone or personal device during lesson time.

Cyberbullying

- I understand that I may not use any communications device, whether personal or provided by the school, for bullying or the harassment of others in any form.
- I will report any issues of cyberbullying to a member of staff as soon as possible, whether it involves myself or others.
- I understand that I should not delete any evidence of cyberbullying, but keep it or take screen shots.
- I understand that a member of staff could ask to see the content of my mobile phone or media device, or confiscate it, if I am involved with any cyberbullying.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that Acceptable Use Policy (AUP) has been understood and agreed.

Pupil

Name: _____ Form: _____

Pupil's Agreement

- I have read, I understand and will abide by the school AUP.
- I will use the computer network, mobile phones, internet access and other new technologies in a responsible way at all times.
- I understand that network and internet access may be monitored.

Signed: _____ Date: _____

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published.

Signed: _____

Parent's Consent for Internet Access

I have read and understood the school AUP and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I also acknowledge that the school is not responsible for the content of the material which is to be found on the internet.

Signed: _____ Date: _____

Please print name _____

Please complete, sign and return to your son/daughter's form teacher.

West Monmouth School

ICT / Information Systems Acceptable Use Agreement

Staff / Adult Users

To ensure that members of staff and other adult users are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Acceptable Use Policy (found in the shared area) for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones; PDAs; digital cameras; external storage devices (e.g. usb hard drives); e-mail and social networking and that only school approved ICT equipment should be used for school business.
- I will not transfer pictures of pupils on to private devices.
- Any photographs/video taken of pupils or staff and use of afterwards will be done with their permission.
- Any images or video footage of pupils will be removed from personal devices (if used) before leaving school and will not be processed, edited or opened on a personal computer at home.
- I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I will not use my mobile phone or personal device for anything other than school purposes during lesson time and when on duty.
- I will use and allow pupils to use school ICT equipment and devices for school purposes only with my direction and guidance.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will not use my school email address to sign up for any social networking sites or other sites other than those used within my professional role.
- I will not open any attachments, using my school email address, from any unknown sources.
- I will respect system security and I will not disclose any password or security information to anyone.
- I will not attempt to bypass any computer or network security settings.
- I will not install any software or hardware without permission from the Head Teacher (via the system administrator – Mr. A Davies).
- I will report any technical issues/viruses or damage to equipment following school procedures as soon as possible.
- I will store only school related or educational data, files and images on the school network and /or VLE.
- I will ensure that personal data is password protected and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property right and adhere to the Data Protection Act 1998.
- I will follow the procedures set by the school's behaviour policy.
- I will advise pupils to keep evidence of any cyber bullying by taking screen shots, saving emails and texts.
- I understand that I can request to view a pupil's personal mobile phone or media device to determine cases of bullying or abuse where the text or image is visible on the device. I understand that the Designated Child Protection Officer is legally able to search a pupil's mobile phone or personal media device to determine a case of bullying or abuse.
- I will report any incidents of concern regarding children's e-safety to the Designated Child Protection Officer or Head Teacher.

- I will ensure that electronic communications with pupils, including email, instant messaging and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will delete old and unnecessary files when required to do so.
- I will not knowingly communicate with pupils via social networking sites.
- I will ensure my social network privacy settings prevent others viewing my personal details and materials and ensure that I never accept or request invites or friend requests from any pupils online.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Breach of this policy will be considered a disciplinary matter.

I have read, understood and accept the Staff Acceptable Use Policy for ICT.

Name	
Signature	
Date	