
# ***Internet Access and Acceptable Use Policy***

***Introduction***
Gwenfo Church In Wales School will allow pupils, teachers, other employees and the community access to its computers, network services, and the Internet.

All pupil activity, when using the network and Internet in school, must be in support of education and/or research and must be appropriate to the educational objectives of the School. Pupils who access the Internet from the school site are responsible for everything that takes place on their computers and all Internet activity is logged.

***Benefits*; -** Access to e-mail and the Internet will enable staff and pupils to

- explore thousands of libraries, databases, museums, and other repositories of information;
- exchange personal communication with other Internet users around the world;
- be included in Government initiatives and global educational projects;
- keep abreast of news and current events;
- take part in discussions with experts;
- publish and display work by creating personal web pages and multimedia presentations.

***Effective Use*; -** Internet access will be planned to enrich and extend learning activities as an integral aspect of the curriculum.

Pupils will

- be given clear objectives of internet use.
- be educated in responsible and effective internet use.
- be supervised appropriately.
- learn to search for and discriminate between valid and inappropriate material.

- learn to copy, save and use material found on the internet without infringing copyright.

***Safety***

Internet access at Gwenfo is filtered by our Internet Service Provider (ISP) and guidelines and procedures are followed within Gwenfo Primary School, but the responsibility of parents and guardians of minors are also considered in conveying the standards that their children should follow when using media and information sources. We also have secondary filtering provided by individual settings specific for each computer. This provides additional customisable filtering which allows the children to only view pages that have been identified as appropriate.

All Web activity is logged so that pupil's activity can be monitored.

***Personal Security Guidelines***

Pupils should

- never reveal personal information, either their own or others, such as home addresses, telephone numbers and personal email addresses.
- not use photographs of themselves on their web pages unless the parent or guardian has given permission to do so.
- never meet people in person that they have contacted on the internet without parent/guardian permission.
- notify their teacher whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.
- be aware that the author of an email or web page may not be the person they claim to be.

***Managing Email***

Email addresses of pupils are not advertised publicly. Each child receiving email is encouraged to reply promptly.

***School and Personal Web Pages***

Pupils are encouraged to take an active role in writing web pages. This often inspires pupils to publish work to a high standard for a wide and varied audience.

Web pages can be used to

- document curricular research.
- be part of an online project.
- promote the school and community.
- publish resources for projects and homework.
- create personal pages detailing interests and displays of work.

***Access Permission***

Pupils are responsible for appropriate behaviour on the school's computer network just as they are in the classroom or on the school playground.

***Parental Support***

Pupils could potentially have unfiltered, unsupervised internet access at home. All parents should be aware of the concerns and benefits of internet use. Parents are therefore encouraged to come in to school to work alongside the teacher to experience the internet first hand and to help in the supervision of the children. The school will also be running some after school internet training sessions to cover the basics of internet use and e-safety.

***Usage Rules and Guidelines***

- Teachers and staff may review documents and log files to ensure that pupils are using the system responsibly.
- Pupils should never download, load or install any software, shareware, or freeware, or load any such software from disks or other sources, unless they have permission from their teacher. Pupils may not copy other people's work or intrude into other people's files without permission.
- Profane, abusive or impolite language should not be used to communicate nor should materials be accessed which are not in line with the rules of school behaviour. A good rule to follow is never view, send, or access materials that you would not want your teachers or parents to see. Should pupils encounter such material, they should immediately report it to their teacher. Children are only allowed in chat rooms with teacher permission, and the ISP has been set to filter out the possibility for us to participate in this facility. No internet games may be played during school hours unless they are approved for educational purposes.
- The pupils should never use the computers to engage in activities that may be in violation of the law.

***Acceptable Use***

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the Internet or the school's Intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

***Personal Responsibility***

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the headteacher via an appropriate method.

***Acceptable Use***

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but as identified earlier in the document together with the following list provides some guidelines on the matter:

***Network Etiquette and Privacy***

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact headteacher.

6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or students finding unsuitable websites through the school network should report the web address to the headteacher.
10. Do not introduce floppy disks or "pen drives" into the network without having them checked for viruses.
11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity. All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
13. Files held on the school's network will be regularly checked by ICT Co-ordinator then results reported to the headteacher.
14. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

***Unacceptable Use***

Examples of unacceptable use include but are not limited to the following:

- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.

- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

***Additional guidelines***

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the ICT Co-ordinator.

***Network Security***

Users are expected to inform ICT Co-ordinator immediately if a security problem is identified. Do not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network.

***Physical Security***

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically stored or protected by locks and or alarms.

***Wilful Damage***

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

***Media Publications***

Written permission from parents or carers will be obtained before photographs of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- the school website / VLE,
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Newspapers.

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given. Parental consent for this as well as other parental agreement and policy information can be obtained from the school office. All parents will need to respond to this document, with the understanding that they are aware of all the issues concerning internet access and acceptable use within Gwenfo Primary School.

This policy will adhere to the Vale of Glamorgan e-safety guidelines and will be updated as and when required when changes to guidelines and conditions are required.

Please return the slip below to the school, although please keep the copy of the policy for your information.

_____

**Parental Agreement**

As a parent/guardian I have read the above policy for access to the internet and use of the school computer equipment and network and agree to abide by its guidelines and conditions.

Signature of parent/guardian: _____ Date: _____

Print Child's Name_____