Internet safety for pupils and staff

POLICY FOR THE SAFE AND ACCEPTABLE USE OF ICT RESOURCES AND THE INTERNET
GUIDELINES FOR **STAFF, GOVERNORS, SUPPLY TEACHERS AND VOLUNTEERS**

For purposes of this policy, "staff" refers to adults visiting or working within the school.

General
It is the responsibility of the staff is to familiarise himself/herself with and abide by the rules of this Acceptable Use Policy and all other applicable school policies.

E-safety is a whole school issue and it is important that there is consistency in the way children and staff are safeguarded from the potential dangers of inappropriate use of ICT.

Mobile Phones
- It is not advisable for staff to give personal mobile phone numbers to children or parents.
- Mobile phones, or any device with video, camera or other media capability, should not be used to take images of children or staff without the agreement of the other party.
- All mobile phones must be switched to silent at the start of the school day. Mobile phones may be used during playtime and dinner when off duty.

Computer Equipment
- All computers, including laptops that are issued to staff, and associated equipment are the property of Ysgol Gellifor / Bryn Clwyd and should be used for **educational purposes only**.
- All installed software MUST be covered by a valid licence agreement held by the School.
- All software installation MUST only be carried out by the ICT technician.
- If you have to leave your laptop unattended during a lesson, either log out or lock it by using the CTRL-ALT-delete keys and then choosing 'Lock Computer'. Once this is done you will need to re-enter your password to gain access.

The Use of Printing Equipment
- Printing and photocopying equipment is provided only for school-related activities. It is recognised that a small amount of personal use may take place but frequent and heavy usage is not permitted.
- The school aims to reduce the environmental and cost impact of printing and staff should note the following guidance;
    - Colour printing typically costs 10 times that of black only printing and should therefore only be used where the use of colour is absolutely necessary to enhance understanding of a document.
    - Print on both sides of the paper wherever facilities exist to reduce the environmental impact and costs.

Internet

All internet access is subject to filtering and content control, to minimise access to inappropriate material.

- Access to websites of an inappropriate nature using the school network, either with school ICT hardware or personal hardware, is forbidden.
- **Staff who access a website of an inappropriate nature should inform the ICT Subject Leader immediately**, if unavailable, a member of the senior management team should be informed. **This has to be officially recorded**.
- The school reserves the right to carry out general checks to ensure appropriate use of facilities including internet access. Regular checks may be carried out if inappropriate use has been suspected.
- Inappropriate use includes browsing, accessing, storing and disseminating material that is:-
    - Illegal (including sites encouraging unlawful activity)
    - Obscene or deliberately offensive in nature
    - Discriminatory (on the grounds of age, disability, faith or belief, gender, race or sexual orientation)
    - Likely to result in harassment or bullying of others
- Staff involved in inappropriate use of facilities including internet use will be disciplined and if illegal behaviour is suspected, the school has a duty to consult with the police.
- ALL internet access is logged and actively monitored and traceable.
- Staff are strongly advised that students should not be part of a member of staff's social networking group e.g. Facebook Friends.

Email

- Personal e-mail accounts should only be accessed on school computers and laptops for work related matters. Work related emails can be sent from the school email address via the school admin computer.
- When possible any work related e-mails should be via the school's e-mail address.
- The sending or receiving of messages which contain any inappropriate material is strictly forbidden.

In terms of teacher's use of social networking and the web, they must be careful what information is posted due to potential security risks.

The following recommendations should be considered if using social networking websites:

- Only use them if absolutely necessary.
- Use only your name for the profile.
- Do not put your date of birth on the profile.
- Be wary of what photographs you put online of yourself, family or friends.
- Remember you must have their permission to publish.

- Make your profiles 'invite' only and thus only allow people you trust with certainty to view your information.
- Do not post your occupation.
- Do not discuss your work.
- Do not publish photographs taken at your work.
- Do not discuss your political or religious views.
- Be careful what viewpoints you express.
- If you do post anything online be mindful of the fact you could lose total control of it.

School based staff should use these social networking sites wisely and cautiously bearing in mind they should not jeopardise themselves, others or their place of work.

Privacy and Data Protection

- Never reveal your password to anyone else or ask others for their password. If you believe that someone may have discovered your password, then change it *immediately*.
- Never attempt to access files or programmes to which you have not granted authorisation.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with Denbighshire County Council Disciplinary Procedures.

The Governing Body has:

- delegated powers and responsibilities to the Head teacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring policies are made available to parents;
- nominated a link governor to visit the school regularly, to liaise with the Head teacher and to report back to the Governing Body;
- responsibility for the effective implementation, monitoring and evaluation of this policy

The Head teacher will:

- ensure all school personnel, pupils and parents are aware of and comply with this policy;
- work closely with the nominated governor;
- monitor the effectiveness of this policy;
- annually report to the Governing Body on the success and development of this policy

The Nominated Governor will:

- work closely with the Head teacher;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the school is aware of this policy;
- report to the Governing Body every term;
- annually report to the Governing Body on the success and development of this policy

School personnel will:

- comply with all aspects of this policy
- not access social networking sites during the school day;
- not post confidential school information or information about any member of the school personnel on any social networking site;
- not make reference to the school or anyone connected to it when using any social networking site;
- not bring the school into disrepute by making any derogatory, defamatory, discriminatory or offensive comments on any social networking site;
- not make discriminatory or offensive comments about any member of the school personnel on any social networking site;
- be aware that the Governing Body will take the necessary disciplinary action if any member of the school personnel breaches this policy

Parents/carers will:

- be aware of and comply with this policy;
- be asked to take part periodic surveys conducted by the school

Security Measures

We work in conjunction with the Local Authority Code of Practice to ensure that computers and servers comply with all up to date Government regulations and are secure with:

- anti-virus software;
- fire wall software;
- passwords

All school personnel are trained to:

- be discreet and confidential;
- consider the safe and secure positioning of computers;
- back up data;
- turn off computers when not in use;
- remember password access;
- lock filing cabinets and doors to offices;
- shred confidential material;
- clear their desk before they leave school

Taking Action

The action that will be taken if inappropriate use is detected ranges from; informal action through to formal disciplinary action and will depend on the nature of the issue. In the majority of cases, informal action will be most appropriate. There will be some circumstances when formal action may be necessary, in which case a formal investigation

will occur. Disciplinary action may then be appropriate depending on the outcome of the investigation.

Review of this policy
This policy is subject to bi-annual reviews. The school reserves the right to change this policy from time to time as may be deemed necessary. We therefore recommend that you check its content on a regular basis.

POLICY FOR THE SAFE AND ACCEPTABLE USE OF ICT RESOURCES AND THE INTERNET GUIDELINES FOR **PUPILS**

General
Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards.

Computer storage areas and removable storage devices will be treated as school property. Staff may review files and communications to insure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted:
1. Sending or displaying offensive messages or pictures
2. Using obscene language
3. Harassing, insulting or attacking others
4. Damaging computers, computer systems or computer networks
5. Violating copyright laws
6. Using others' passwords
7. Trespassing in others' folders, work or files
8. Intentionally wasting limited resources

Rules

Rules for Responsible Use of ICT resources and the Internet

The school has installed computers with internet access to help our learning.

These rules will keep you safe and help us to be fair to others.

- I will not access another person's user area, or interfere with other people's work or computer files;
- I will use the computers for school work and study work, and not waste computer time other students could find useful;
- I will not behave in a way that can cause damage to ICT equipment or to software installations;
- I will not bring in removable storage devices from outside school unless I have been given permission;
- I will not bring in software from home or make a copy of school software without permission from a member of staff;
- I will ensure I have permission from a member of staff before using the Internet;
- I will only use school E-mail for projects my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;

We will display this page as a poster near computers.

We will provide pupils & parents with a copy of these rules to read.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on internet use or use of the school computers in general.

2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

3. When applicable, police or local authorities may be involved. The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, 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.

Review of this policy

This policy is subject to bi-annual reviews. The school reserves the right to change this policy from time to time as may be deemed necessary. We therefore recommend that you check its content on a regular basis.

Please read this document carefully. Only once you have signed to acknowledge you have read this policy will access to ICT resources and the Internet be permitted.

I have read and understood the above and agree to use the school's ICT resources within these rules.

Presented to staff _____

Date _____

Signed _____

Presented to Governors _____

Signed _____

Next review _____