Ysgol Gymunedol **Llangatwg**
Llangatwg Community School

Main Road | Cadoxton | Neath | SA10 8DB

School E-Safety Policy

Ysbrydoli Dyheu Llwyddo **Inspire Aspire Succeed**

Prifathro/ Headteacher: Mr. Alan. L. Rowlands BA (Hons), PGCE, NPQH
Ffôn/ Tel: (01639) 634700 Ffacs/ Fax: (01639) 634708 Email: llangatwgschool@npted.org

2.1 Who will write and review the policy?

- The school has appointed an e-Safety Coordinator.

- This e-Safety Policy and its implementation will be reviewed annually.

- Our e-Safety Policy has been written by the school, building on the Neath Port Talbot e-safety Policy and government guidance. It has been agreed by the senior management and approved by governors.

2.2 Teaching and learning

2.2.1 Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

- Internet use is part of the statutory curriculum and a necessary tool for learning.

- Internet access is an entitlement for students who show a responsible and mature approach to its use.

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;

- inclusion in the Lifelong Learning Network Wales which connects all schools in NPT;

- educational and cultural exchanges between pupils world-wide;

- vocational, social and leisure use in libraries, clubs and at home;

- access to experts in many fields for pupils and staff;

- professional development for staff through access to national developments, educational materials and effective curriculum practice;

- collaboration across support services and professional associations;

- improved access to technical support including remote management of networks and automatic system updates;

- exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government;

- access to learning wherever and whenever convenient.

2.2.3 How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught and given guidance on what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.4 How will pupils learn how to evaluate Internet content?

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

- The evaluation of on-line materials is a part of every subject.

2.3 Managing Information Systems

2.3.1 How will information systems security be maintained?

- The security of the school information systems will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with NPTCBC.

- The school will work closely with NPTCBC to ensure the safety and integrity of any wireless system used or installed in school.

- School or NPTCBC data should not be stored on personal devices.

o Personal data sent over the Internet will be encrypted or otherwise secured.

o Portable media may not be used without specific permission followed by a virus check.

o Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

o Files held on the school's network will be regularly checked.

o The ICT co-ordinator / network manager will review system capacity regularly.

2.3.2 How will e-mail be managed?

- Pupils may only use approved e-mail accounts.

- Pupils may only send internal email unless additional access permissions have been granted.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- The forwarding of chain letters is not permitted.

o Access in school to external personal e-mail accounts may be blocked.

o Excessive social e-mail use can interfere with learning and may be restricted.

o E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

2.3.3 How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.

o E-mail addresses should be published carefully, to avoid spam harvesting.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images of pupils are electronically published.

- Work can only be published with the permission of the pupil and parents.

2.3.5 How will social networking and personal publishing be managed?

- Social Network sites and newsgroups will be filtered unless a specific use is approved. (Schools have a responsibility to report any additional sites that they need filtered/blocked)

- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name or school.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

- Students should be advised not to publish specific and detailed private thoughts.

- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

2.3.6 How will filtering be managed?

- The school will work with NPTCBC, taking into account Becta guidelines, to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety Coordinator and forwarded to Neath Port Talbot County Council IT service desk immediately.

- All Internet access in the school will be logged

- Internet use will be randomly monitored to ensure compliance with school policy.

- Larger schools, generally secondary, will manage the configuration of their filtering. This task requires both educational and technical experience.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be reported to appropriate agencies.

- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by engineers.

2.3.7 How will videoconferencing be managed?

The equipment and network

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- Equipment connected to Lifelong Learning Network Wales should use the national E.164 numbering system.

- External IP addresses should not be made available to other sites.

- Videoconferencing contact information should not be put on the school Website.

- The equipment must be secure and if necessary locked away when not in use.

- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing should be supervised appropriately for the pupils' age.

- Parents and guardians should agree for their children to take part in videoconferences.

- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.

- Only key members of staff should be given access to the videoconferencing system, web or other remote control page available on larger systems.

- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.

- Recorded material shall be stored securely.

- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

2.3.8 How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school.

2.3.9 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.
- Secondary students must apply for Internet access individually by agreeing to comply with the e-Safety Rules.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

2.4.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor NPTCBC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.3 How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the head teacher.

- Pupils and parents will be informed of the complaints procedure.

o Parents and pupils will need to work in partnership with staff to resolve issues.

o Discussions will be held with the local Community Police Officer to establish procedures for handling potentially illegal issues.

o Sanctions within the school discipline policy include:

o interview/counselling by the Progress Manager;

o informing parents or carers;

o removal of Internet or computer access for a period.

2.4.4 How is the Internet used across the community?

o The school will liaise with local organisations to establish a common approach to e-safety.

o The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

2.5 Communications Policy

2.5.1 How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.

- Pupils will be informed that network and Internet use will be monitored.

- An e-safety programme will be introduced to raise the awareness and importance of safe and responsible internet use.

- Guidelines in responsible and safe use should precede Internet access.

- An e-safety module will be included in the PSE or ICT programmes covering both school and home use.

2.5.2 How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.

o Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

o Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

o Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

2.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.

o Internet issues will be handled sensitively, and parents will be advised accordingly.

o A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

o Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

1. e-Safety Contacts and References

- **e-Safety Officer, NPTCBC**
  Aled Evans – Head of Education, Development and Inclusion Services Tel:

- **BITC Servicedesk**
  Help with filtering and network security. Tel: 01639 779500

- **Children's Safeguards Service**
  Susan Samuel – Manager of Children and Young People's Partnership

BBC Chat Guide	http://www.bbc.co.uk/chatguide/
Becta	http://www.becta.org.uk/schools/esafety
Childline	http://www.childline.org.uk/
Child Exploitation & Online Protection Centre	http://www.ceop.gov.uk
e-Safety in Schools and Schools e-Safety Policy	http://www.clusterweb.org.uk?esafety
Grid Club and the Cyber Cafe	http://www.gridclub.com
Internet Watch Foundation	http://www.iwf.org.uk/

Internet Safety Zone	http://www.internetsafetyzone.com/
Kent Primary Advisory e-Safety Pages	http://www.kented.org.uk/ngfl/ict/safety.htm
Kidsmart	http://www.kidsmart.org.uk/
NCH – The Children's Charity	http://www.nch.org.uk/information/index.php?i=209
NSPCC	http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Stop Text Bully	www.stoptextbully.com
Think U Know website	http://www.thinkuknow.co.uk/
Virtual Global Taskforce – Report Abuse	http://www.virtualglobaltaskforce.com/

2. Supporting Materials

The websites listed in section 3 is by no means exhaustive and can change within the lifetime of this document. The school will direct staff to look at the free resources available on these sites as repitable and up to date guidance and advice - particularly the Childnet International site, thinkuknow.co.uk and the BBC.

3. Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the child to 18 years old;

- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and

- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent : there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);

- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or

- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

4. Acknowledgements

This document is based on e-safety guidance published by Becta and includes statements published by Kent County Council.