E-SAFETY POLICY

NORTH GOWER PARTNERSHIP

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society; both within schools and in their lives outside school.

The internet and other digital information technologies are powerful tools, which open up new opportunities for learning. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all members of the school community, from the headteacher and governors to the senior leaders, classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge

- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Extremism / Terrorism
- Consequences of sharing own images via social media

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is

reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Development/Monitoring/review of this policy

This draft e-safety policy has been developed by the Local Authority and adopted by the school. It will be monitored by the e-safety co-ordinator and reviewed by relevant members of the Governing Body as appropriate.

Further consultation with the whole school community will take place through the following:

- Staff meetings
- School / Student / Pupil Council
- INSET Day
- Governors meeting / subcommittee meeting
- Parents' evenings
- School website / newsletters
- Assemblies
- Social media

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the relevant subcommittee who will receive regular information about e-safety incidents. A member of the Governing Body will take on the role of E-Safety Governor. The role will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting.

Head-teacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and CPD Co-ordinators are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headship Team will receive regular monitoring reports from the E-Safety Co-ordinator, which will be disseminated to the relevant Sub-Groups of the Governing Body.
- The Headteacher and the Child Protection Officer are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff following the appropriate guidance given in the LEA's brochure 'Responding to incidents of misuse' and relevant Local Authority HR/disciplinary procedures, as well as following the 'All Wales Child Protection Procedures'.

The role of the E-Safety Coordinator is to:

- lead the e-safety committee
- take day to day responsibility for e-safety issues and have a leading role in establishing and review the school's e-safety policies and documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attend relevant meeting/committee of Governors
- report regularly to Headship Team

Network Manager / Technical staff:

The Network Manager with the ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SLTS is informed of issues relating to the filtering applied by the County
- The school's filtering policy (if it has one) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that s/he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network, Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher/ICT Co-ordinator/Head of Year (as in the section above) for investigation/action/sanction that monitoring software/systems are implemented and updated as agreed in school policies.
- Obtained consent forms to comply with GDPR laws in order to grant access to HWB, Google Classroom and any other VLE's.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- They comply with the guidelines of the GDPR legislation and inform relevant authority of any breech.
- They report any suspected misuse or problem to the E-Safety Co-ordinator/ Officer/Headteacher/ICT Co-ordinator/Class teacher/Head of Year (as in the section above) for investigation/action/sanction.
- Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students / pupils understand and follow the school's e-safety and acceptable use policy
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection

The person designated should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- Extremism

E-Safety Committee

The ICT working group will work with the E-Safety Co-ordinator on:

- The production / review / monitoring of the school e-safety policy / documents.
- The production/review/monitoring of the school filtering policy
- The consideration and updating of policy if any new legislation is passed

Students/pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these

issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.
- endorsing (by signature) the use of named applications e.g. HWB / Google in accordance with GDPR legislation.

Community Users and Visitors

Community and visitor Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Status

Draft:	December 2009	
For Introduction	January 2010	
Previous Review	January 2015	
Current Review	July 2019	Reviewed By: NGP DCF co-ordinators and Governors