E-Safety Policy

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 and information technologies are powerful tools, which open up new opportunities for everyone. 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. An E-Safety Policy should help to ensure safe and appropriate use.

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

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 to help ensure 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 we intend to do this, while 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 communications technologies for educational, personal and recreational use.

Development, Monitoring & Review of this Policy

This E-Safety Policy has been developed by:

- Catherine Kucia – Deputy Headteacher
- Robert Aspinall – TLR Digital Learning

In consultation with:

- Pupils
- Teachers
- Support Staff
- Governors
- Parents and Carers

Schedule for Development, Monitoring & Review

This E-Safety Policy was approved by the Governing Body on:	5th May 2016
The implementation of this E-Safety Policy will be monitored by:	Catherine Kucia Robert Aspinall Ian Cole – Governor
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of this E-Safety Policy:	Termly
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	January 2017
Should serious e-safety incidents take place, the following external agencies will be informed:	Nicola Davies – LA Safeguarding Officer Newport Police Child Protection Team

The school will monitor the impact of the policy using:

- ESafety Log – located in CK's Office
- Internal monitoring data for network activity
- Monitoring of SIMS Records of Discrimination
- Surveys of pupils (e.g., CEOP survey www.thinkuknow.co.uk)
- Surveys of staff
- Information for parents/carers

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.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Debbie Private is the named Governor responsible for Child Protection, which includes E-Safety.

Headteacher and LAST

The Headteacher is responsible for ensuring the safety, including e-safety, of members of the school community. The Headteacher is the named Child Protection Officer, which includes a responsibility for e-safety.

The Headteacher and LAST are responsible for:

- Leading our school e-safety initiative
- Taking day-to-day responsibility of e-safety issues and log any incidents
- Ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues
- Following correct procedure in the event of a serious e-safety allegation being made against a member of staff

Network Manager – Newport LA STEP Team

The school's ICT is managed by Newport LA STEP Team. They are responsible for:

- Ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance
- Ensuring that users may only access the school's networks through a properly enforced password protection policy
- Ensuring that the use of the network, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher

Teaching and Support Staff

All staff are responsible for:

- Ensuring that they have an up to date awareness of e-safety matters
- Reading and adhering to the school's e-safety policy and practices
- Reading, understanding and signing the school Staff Acceptable Use Policy
- Reporting any suspected misuse or problem to the Headteacher or Catherine Kucia
- Ensuring any digital communications with pupils are on a professional level and only carried out using official school systems
- Ensuring that E-safety issues are embedded in all aspects of the curriculum and other school activities
- Ensuring that pupils understand and follow the school e-safety and acceptable use policy
- Monitoring ICT activity in lessons and extended school activities
- Teaching children so that they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Ensuring pupils 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
- Using suitable internet sites during planned lessons

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy
- 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 know and understand school policies on the taking/use of images and on cyber-bullying
- They 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

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided, which will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems and the internet will be posted in all rooms
- All staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet and 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 meetings, newsletters, letters, website and information about national and local e-safety campaigns.

Parents and carers will be responsible for:

- Endorsing the Pupil Acceptable Use Policy for pupils.
- Accessing the school website in accordance with the relevant school Acceptable Use Policy.

The school will offer family learning courses in ICT and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users

Community Users who access school ICT systems as part of the extended school provision will be expected to sign a Community User AUP before being provided with access to school systems.

Technical – infrastructure, equipment, filtering and monitoring

Newport STEP team will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All classes will be provided with a class log-on by Bob Aspinall. All staff must be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP.
- Members of staff should never use a class log on for their own network access.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet, e.g., on social networking sites.

Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs. General photographic permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software

ESafety Education & Training
Education – Pupils
ESafety education will be provided in the following ways:

- A planned e-safety programme which covers the use of ICT and new technologies both inside and outside school
- Key e-safety messages reinforced as part of a planned programme of assemblies
- In all lessons using ICT, pupils are taught to be critically aware of the materials and content they access online

Education & Training – Staff
All staff receive e-safety training and understand their responsibilities as outlined in this policy. E-Safety is an integral part of new staff induction.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks:

	Staff & Other Adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other personal camera devices				✓				✓
Use of hand held devices e.g., PDAs, PSPs	✓				✓			
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails		✓						✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs	✓						✓	

Pupils in Y5 & Y6 are allowed to bring mobile phones into school, with staff permission. These phones must be taken to the school office for safe keeping during the school day. Mobile phones brought to school are entirely at their owners risk and Glan Usk Primary School does not accept any responsibility for any loss or damage.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Staff and pupils should therefore use only the school email service to communicate with others when in school or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public social networking programmes must not be used for these communications

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Unsuitable and Inappropriate Activities

Some Internet activity, e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures as follows:

Staff **Actions/Sanctions**

Incidents:	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for Action re filtering etc	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal				✓				✓
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email during school time		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓						
Careless use of personal data, e.g., holding or transferring data in an insecure manner		✓						
Deliberate actions to breach data protection or network security rules		✓				✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓		✓		✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓						
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with pupil		✓				✓		
Actions which could compromise the staff member's professional standing	✓	✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓						
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓			
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				✓
Breaching copyright or licensing regulations		✓						
Continued infringements of the above, following previous warnings or sanctions								✓

Pupils

Actions/Sanctions

Incidents:	**Refer to Class Teacher**	**Refer to LAST**	**Refer to Headteacher**	**Refer to Police**	**Refer to technical support for action**	**Inform parents/carers**	**Removal of network access rights**	**Warning**	**Further sanction, e.g., exclusion**
Deliberately accessing or trying to access material that could be considered illegal			✓	✓		✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone/digital camera/other handheld device	✓								
Unauthorised use of social networking/instant messaging/personal email		✓	✓						
Unauthorised downloading or uploading of files	✓								
Allowing others to access school network by sharing username and passwords	✓								
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓						
Corrupting or destroying the data of other users		✓	✓						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions									✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓				
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓				
Deliberately accessing or trying to access offensive or pornographic material				✓		✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓						