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

Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by a working group made up of:

- *Junior and Infant e-Safety Coordinators (M. Evans, L. Griffiths and D. Nevitt)*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*Spring 2019*
The implementation of this e-Safety policy will be monitored by the:	*e-Safety Coordinators*
Monitoring will take place at regular intervals:	Annually
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
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:	Spring 2023
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, PC Mark Jones, Police (depending on the incident)

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of*
    - *students / pupils*
    - parents / carers
    - *staff*

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals[1] 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 *Governing body* receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor[2] to include:

- *regular meetings with the e-Safety Co-ordinators*
- *regular monitoring of e-Safety incident logs*
- *reporting to Governors*

Headteacher / Principal and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community**, though the day to day responsibility for e-Safety may be delegated to the *e-Safety Co-ordinators.*
- **The Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.**[3]
- *The Headteacher / Principal / Senior Leaders are responsible for ensuring that the e-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.*

e-Safety Coordinators (ME, LG and DN):

The *e-Safety Coordinators*

- lead the e-Safety committee
- take day to day responsibility for e-Safety issues and review the school e-Safety policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provide (or identifies sources of) training and advice for staff
- liaise with technical staff

Technical staff (Flintshire LEA):

The *Technical Staff* are responsible for ensuring:

- **that Ysgol Mynydd Isa's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**

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 Staff Acceptable Use Policy**
- **they report any suspected misuse or problem to the *Headteacher* for investigation / action**

[1] In a small school some of the roles described below may be combined, though it is important to ensure that there is sufficient "separation of responsibility" should this be the case.
[2] It is suggested that the role may be combined with that of the Safeguarding Governor
[3] see flow chart on dealing with e-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures.

- **all digital communications with pupils and parents should be on a professional level**
- **e-Safety issues are embedded in all aspects of the curriculum and other activities**
- **pupils understand and follow the e-Safety and acceptable use *agreement***
- **pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations**
- **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**

Safeguarding Designated Person (RC or SS/EC if RC unavailable):

The Safeguarding Designated Person should be trained in e-Safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data[4]
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

e-Safety Committee

Members of the e-Safety Committee will assist the e-Safety Coordinators and SLT with:

- the monitoring of the school e-Safety policy.
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression.
- consulting stakeholders – including parents and pupils about the e-Safety provision.

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement**
- **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**
- **should understand the importance of adopting good e-Safety practice when using digital technologies out of 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about e-Safety*.* Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events e.g. assemblies, sporting events, trips and concerts
- access to parents' sections of the school website, Social Media and Class Dojo

Policy Statements

Education – young people

[4] Appendix B2

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-Safety curriculum should be provided and key e-Safety messages should be reinforced as part of a planned programme of assemblies and PSE programme.**
- **Pupils should be taught in all lessons to be critically aware of content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.**
- **Pupils should access a range of activities through e-aware and other sources, e.g. Common Sense media and CEOP.**

Education & Training – Staff / Volunteers

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **e-Safety training will be made available to staff.**
- **All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.**

Training – Governors

Governors should take part in e-Safety training.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Internet access is filtered for all users.**

Use of digital and video images

- **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 eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

- Care should be taken when taking digital / video images that students / 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

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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

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, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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 / disadvantages:

Staff & other adults	Students / Pupils

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	owed with staff permission	Not allowed
Use of mobile phones in school		🟩		🟥				
Use of mobile phones in lessons		🟩		🟥				
Use of mobile phones in social time		🟩		🟥				
Taking photos on mobile phones / cameras		🟩		🟥				
Use of other mobile devices eg tablets, gaming devices, smart watches		🟩		🟥				
Use of personal email addresses (excluding Hwb email adresses) in school, or on school network		🟩		🟥				
Use of school email for personal emails		🟩		🟥				
Use of messaging apps		🟩		🟥				
Use of social media (personal accounts)		🟩		🟥				
Use of blogs (personal accounts)		🟩		🟥				

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. Users should be aware that email communications are monitored.
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / 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 social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.* (Schools may choose to use group or class email addresses for younger age groups eg. at KS1)
- *Students / pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out by the General Workforce Council (GWC) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	

remarks, proposals or comments that contain or relate to:	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube			X			

(The school should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their own responses)

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.