

E-Safety Policy

ADOPTED ON : 07/06/2017

Signed by Chair of Governors

A handwritten signature in black ink, appearing to read 'J. Stannard', is written over a faint horizontal line.

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:

- *Headteacher*
- *e-Safety Officer / Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*

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 <i>Governing Body / Governors Sub Committee</i> on:	
The implementation of this e-Safety policy will be monitored by the:	<i>e-Safety Coordinator, Committee, Senior Leadership Team)</i>
Monitoring will take place at regular intervals:	Annually
The <i>Governing Body / Governors Sub Committee</i> 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:	<i>Termly meeting if incidents occur</i>
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:	
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	<i>LA ICT Manager, LA Safeguarding Officer, Police</i>

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
 - *students / pupils*
 - *parents / carers*
 - *staff*

Contents

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals¹ 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 / Governor's sub-committee* receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor² to include:

- *regular meetings with the e-Safety Co-ordinator / Officer*
- *regular monitoring of e-Safety incident logs*
- *regular monitoring of filtering / change control logs (where possible)*
- *reporting to relevant Governors / sub-committee / meeting*

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-ordinator / Officer.**
- **The Headteacher and another member of the Senior Leadership Team / 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 is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training 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 Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator / Officer.**

e-Safety Coordinator / Officer:

The *e-Safety Coordinator / Officer*

- leads the e-Safety committee
 - takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
 - ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
 - provides (or identifies sources of) training and advice for staff
 - liaises with the Local Authority / relevant body
 - liaises with (school) technical staff
 - receives reports of e-Safety incidents⁴ and creates a log of incidents to inform future e-Safety developments.
 - meets regularly with e-Safety *Governor* to discuss current issues, review incident logs and if possible, filtering / change control logs
-

- attends relevant meeting / sub-committee of *Governors* reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The *Network Manager / Technical Staff* (or managed service provider) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the required e-Safety technical requirements as identified by the Local Authority or other relevant body and also the e-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that they keep 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; e-Safety Coordinator / Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

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 / Agreement they report any suspected misuse or problem to the *Headteacher; e-Safety Coordinator / Officer* for investigation / action
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems unless permission has been given by the e-safety officer, senior management
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-Safety and acceptable use agreements / policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches are reported directly to the e-safety officer.

Safeguarding Designated Person

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 data⁵
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The e-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and monitoring the e-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the *e-Safety Coordinator / Officer* with:

- the production / review / monitoring of the school e-Safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / carers and the students / pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool

An e-Safety Group Terms of Reference Template can be found in the appendices (B4)

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand 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. The school will take every opportunity to help parents understand these issues through newsletters, letters, website / VLE and information about national / local e-Safety campaigns / literature. 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
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. ([A Community Users Acceptable Use Agreement Template can be found in the appendices \(A5\)](#))

Policy Statements

Education – young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / 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 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 as part of ICT / Computing / PSE / DCF lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies activities
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students / 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.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- Campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg <https://hwb.wales.gov.uk/>
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-Safety knowledge and experience. This may be offered through the following:

- e-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school VLE / website will provide e-Safety information for the wider community

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:

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify e-Safety as a training need within the performance management process.*
- 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.
- The e-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / e-Safety / health and safety / safeguarding . This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues if the service is not provided by the Authority.

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 which is provided by the LEA.
- 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
- All users will have clearly defined access rights to school technical systems and devices.
- All users of HWB will be provided with a username and secure password. Users are responsible for the security of their username and password
- Username and secure passwords will be provided for staff and individual classrooms and staff passwords will be changed every 30 days.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g school safety cabinet)
- [Head teacher](#) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider LEA. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering [changes](#)
- An appropriate system is in place (log book is kept in office and is reported immediately to IT Centre) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). (Appendix C2)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place ([See Appendix B3](#)) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place ([See Appendix B3](#)) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place ([see appendix B2](#)) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. ([see appendix B2](#))

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD must not introduce vulnerabilities into existing secure environments.

A device may be a privately owned smartphone, tablet, notebook / laptop or other new technology that usually has the capability of utilizing the school's wireless network. The device then has access to the wider internet including the school's (Hwb+) learning platform and other cloud based services such as email and data storage. The device may typically also be used for the taking of images, for the recording of sounds or video and for generating and storing a wide range of other types of data (often as a result of using an app).

The absolute key to approaching BYOD is that the students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device they use is user or school owned. This understanding then underpins further conventions around acceptable use of both the devices and of the wider network.

Potential Benefits of BYOD

Research is highlighting the widespread uptake of portable, wireless enabled electronic devices amongst adults and children of all ages. This technology exists as part of their everyday digital world and by allowing them to use these devices freely in school, the school is bringing that familiar digital life into the school classroom. Learners will no longer have to 'power down' when they walk through the doors of the school and can engage with and own their learning more effectively. BYOD has the potential to maximise the huge investments that have been made in schools' infrastructure and allows for greater opportunity to engage with learning technologies.

Considerations

Schools do need to be aware that access to such devices is not yet ubiquitous and that any BYOD implementation will need to address issues over equality of access for all learners.

BYOD brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement BYOD successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

The school must develop a new, strengthened Acceptable Use Agreement for staff, students and parents/carers as a minimum, and will need to support teaching staff, learners and parents through this shift in approach.

The essential principle of safe and responsible use of the internet and learning technologies sits with the understanding that this technology is allowed primarily for educational purposes. Online safety should already be enshrined in existing e-Safety awareness programmes and in the school's current Acceptable Use documentation. The BYOD policy should sit alongside a range of policies including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use (of the internet) Policy, policies around theft or malicious damage and the Behaviour Policy.

(see appendix B3 for a more detailed BYOD Policy)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / 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.
- 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 is 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.
- Staff and volunteers are allowed to take digital / 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 **unless permission is given by school**.
- 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.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Parents / Carers Acceptable Use Agreement in the appendix)
- Student's / Pupil's work can only be published with 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 be 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

The Personal Data Handling Policy Template in appendix B2 provides more detailed guidance on the school's responsibilities and on good practice.

Communications

This is an area of rapidly developing technologies and uses. School will need to discuss and agree how they intend to implement and use these technologies, e.g. few school allow learners to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the learners. The table has been left blank for school to choose its own responses.

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			Learners				
	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/cameras								
Use of other mobile devices eg tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

Communication Technologies

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

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. Staff and learners should therefore use only the school email service to communicate with others when in school, or on school systems, (e.g. by remote access).**
- **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 learners or parents/carers (email, chat, learning platform, 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 learners at KS2 and above will be provided with individual school email addresses for educational use (HWB)**
- **Learners should be taught about online 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

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) 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 school and local authorities have a duty of care to provide a safe learning environment for pupils and staff. School 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 learners 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 through:

- Ensuring that personal information is not published
- Training is provided including: 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 learners, parents and 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.

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

School use of social media for professional purposes will be checked regularly by the senior risk officer and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

[The social media policy template in appendix B4 provides more detailed guidance on the school's responsibilities and on good practice.](#)

Unsuitable/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 technical systems. Other activities, e.g. online 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, or out of, school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

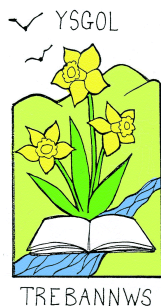
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				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, (e.g. 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	
Online gaming (educational)		x				
Online gaming (non educational)			x			
Online gambling					x	
Online shopping/commerce				x		
File sharing			x			
Use of social media			x			
Use of messaging apps			x			
Use of video broadcasting, e.g. YouTube				x		

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 (Appendix C1)



Ysgol Gynradd Gymraeg Trebannws
Trebannws Welsh Primary School
Pennaeth/Headteacher: Mrs R.Evans



A1 Student / Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

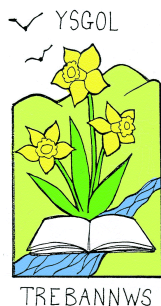
I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):.....



Ysgol Gynradd Gymraeg Trebannws
Trebannws Welsh Primary School
Pennaeth/Headteacher: Mrs R.Evans



A2 Student / Pupil Acceptable Use Agreement (AUA)

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a

member of staff to do so. (schools should amend this section to take account of their policy on each of these issues)

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal device(s) in school if I have permission I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

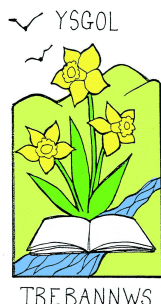
Name of Student / Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature



Ysgol Gynradd Gymraeg Trebannws

Trebannws Welsh Primary School

Pennaeth/Headteacher: Mrs R.Evans



A4 Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet, HWB and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet, HWB and to ICT systems at school.

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

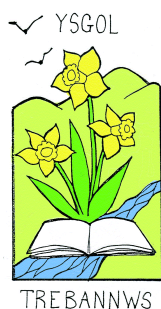
I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed

Date



Ysgol Gynradd Gymraeg Trebannws

Trebannws Welsh Primary School

Pennaeth/Headteacher: Mrs R. Evans



A5 - Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

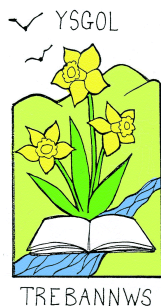
- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices
- **Devices that are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user and their parents/carers as does the liability for any loss or damage resulting from the use of the device in school.**
- **The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school.**
- **The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network.**
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date



Ysgol Gynradd Gymraeg Trebannws
Trebannws Welsh Primary School
Pennaeth/Headteacher: Mrs R.Evans



B2 School Personal Data Handling Policy

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements

The school 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". (see Privacy Notice section below)

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is **Mrs Rhian Evans**. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) **(the school may wish to identify these staff by name or title in this section)** for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration – Reg ref: Z6971189

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

: http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through Prospectus, newsletters, reports or a specific letters. Parents / carers of young people who are new to the school will be provided with the privacy notice through (prospectus, consent form etc).

More information about the suggested wording of privacy notices can be found on the WG website.

Training & awareness

All staff will be made aware of their responsibilities in data handling/ data awareness / data protection as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Schools will need to review the above section with regard to LA policies (where relevant), which may be more specific, particularly in the case of HR records.

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly (monthly). User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media) Private equipment (i.e owned by the users) must not be used for the storage of personal data.

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 and 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.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (LA Baglan – back up data every night)

The school has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Office365) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (see appendix for further information and the ICO Guidance:

http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx)

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (NB. to carry encrypted material is illegal in some countries)

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

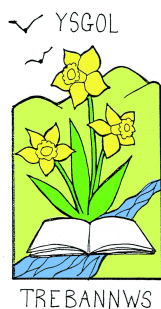
Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the “Data Handling Procedures in Government” document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by Mrs Evans. The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: [\(schools should determine their own reporting policy, in line with that of their LA \(if relevant\), and add details here\)](#)

- a “responsible person” for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.



Ysgol Gynradd Gymraeg Trebannws Trebannws Welsh Primary School

Pennaeth/Headteacher: Mrs R.Evans



B3 School Mobile Technologies Policy Template (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreement, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

A policy that completely prohibits pupil/student, staff or visitors from bringing mobile technologies to the school/academy could be considered to be unreasonable and unrealistic for school/academy to achieve. For example many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone and many staff and visitors use mobile phones to stay in touch with family. Contractors require mobile technologies for legitimate business reasons.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: <http://education.alberta.ca/admin/technology/research.aspx> and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - <http://www.nen.gov.uk/bring-your-own-device-byod/>

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school/ network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding

potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- The school has provided technical solutions for the safe use of mobile technology for school devices and for personal devices
- For all mobile technologies, filtering will be applied to the school internet connection and attempts to bypass this are not permitted
- Where mobile broadband (e.g. 3G and 4G) use is allowed in the school, users are required to follow the same acceptable use requirements as they would if using school owned devices.
- Mobile technologies must only be used in accordance with the law
- Mobile technologies are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
- Learners will be educated in the safe and appropriate use of mobile technologies as part of the online safety curriculum
- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device ⁶	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	no	no	no
Internet only	Yes	Yes	Yes	no	no	no
No network access						

School devices

- All school devices are controlled through the use of mobile device management (MDM) software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. internet only access, network access allowed, shared folder network access)
- All school devices must be suitably protected via a passcode/password/pin (and encryption where relevant). Those devices allocated to members of staff must only be accessed and used by members of staff
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain their property and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs
- The school is responsible for keeping devices up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network. Where user intervention or support for this process is required, this will be made clear to the user
- School devices are provided to support learning.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended is not permitted
- *All school devices are subject to routine monitoring*

Personal devices

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the school
- Staff personal devices should not be used to contact learners or their families, nor should they be used to take images of learners unless permission is given by e-safety officer

- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day

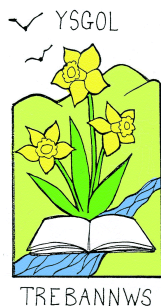
User behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy
- Guidance is made available by the school to users concerning where and when mobile devices may be used
- Devices may not be used in tests or exams
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Devices must be in silent mode on the school site and on school buses
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Learners must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, except in emergency situations
- Printing from personal devices will not be possible

Visitors

Visitors will be provided with information about how, where and when they are permitted to use mobile technology on the site, in line with local safeguarding arrangements. They will also be informed about the school policy on taking images.



Ysgol Gynradd Gymraeg Trebannws
Trebannws Welsh Primary School
Pennaeth/Headteacher: Mrs R.Evans



B4 School Policy - e-Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and the monitoring of the e-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Full Governing Body.

2. MEMBERSHIP

2.1 The e-Safety committee will seek to include representation from all stakeholders.
The composition of the group should include *(NB in small schools one member of staff may hold more than one of these posts):* [add/delete where appropriate]

- Safeguarding officer – Rhian Evans
- Teaching staff member – Amy Grinter
- Support staff member – Rebecca Morris
- e-Safety coordinator – Rhian Evans and Amy Grinter
- Governor – Neil Harper
- Parent / Carer
- Digital Wizards – for advice and feedback. Students / pupils are only expected to take part in committee meetings where deemed relevant.

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly for a period of roughly 1 hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the e-Safety Co-ordinator (or other relevant person) with the following:

- To annually review and develop the e-Safety policy in line with new technologies and incidents

- To monitor the delivery and impact of the e-Safety policy
- To monitor the log of reported e-Safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-Safety. This could be carried out through:
 - Staff meetings
 - Student / pupil forums (for advice and feedback)
 - Governors meetings
 - Parents evenings
 - Website/VLE/Newsletters
 - Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for YGG Trebannws have been agreed

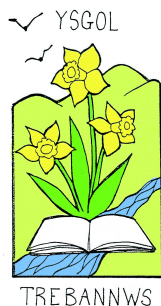
Signed by (SLT):

Date:

Date for review:

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council



Ysgol Gynradd Gymraeg Trebannws

Trebannws Welsh Primary School

Pennaeth/Headteacher: Mrs R.Evans



B5 Social Media Template Policy

Social media (e.g. Facebook, Twitter) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents and carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school its staff, parents and carers and learners.

Scope

This policy is subject to the school codes of conduct and acceptable use agreements.

This policy:

- applies to all staff and to all online communications which directly or indirectly, represent the school.
- applies to such online communications posted at any time and from anywhere.
- encourages the safe and responsible use of social media through training and education
- *defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- SLT
 - facilitating training and guidance on Social Media use.
 - developing and implementing the Social Media policy
 - taking a lead role in investigating any reported incidents.
 - making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - receive completed applications for Social Media accounts
 - approve account creation
- Administrator / Moderator
 - create the account following SLT approval
 - store account details, including passwords securely
 - be involved in monitoring and contributing to the account
 - control the process for managing an account after the lead staff member has left the school (closing or transferring)
- Staff
 - know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - attending appropriate training
 - regularly monitoring, updating and managing content he/she has posted via school accounts
 - adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

 - the aim of the account
 - the intended audience
 - how the account will be promoted
 - who will run the account (Mrs Evans and Mrs Bevan)
 - will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next

working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
 - engaging
 - conversational
 - informative
 - friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
- **permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected
- **under no circumstances should staff share or upload learner pictures online other than via school owned social media accounts**
- staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published
- if a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

- personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in the school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to private social media sites.

Pupil/Students

- Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media network account

- the school's education programme should enable the learners to be safe and responsible users of social media
- learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use
- The school has an active parent and carer education programme which supports the safe and positive use of social media. This includes information on the website
- parents and carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- “nothing” on social media is truly private
- social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- check your settings regularly and test your privacy
- keep an eye on your digital footprint
- keep your personal information private
- regularly review your connections – keep them to those you want to be connected to
- when posting online consider; Scale, Audience and Permanency of what you post
- if you want to criticise, do it politely
- take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- know how to report a problem

Managing school social media accounts

The Do's

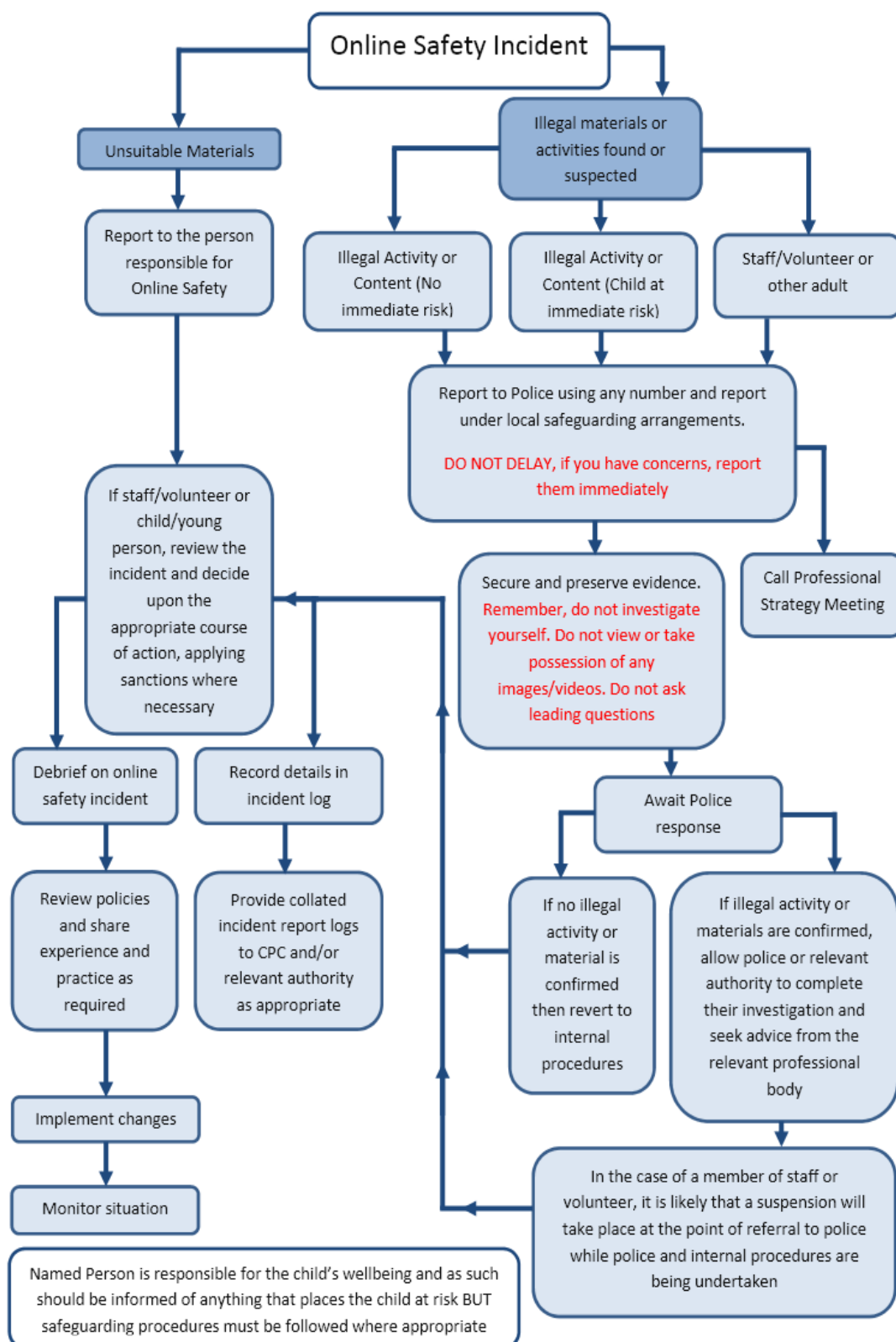
- Check with a senior leader before publishing content that may have controversial implications for the school
- use a disclaimer when expressing personal views
- make it clear who is posting content
- use an appropriate and professional tone
- be respectful to all parties

- ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
- express opinions but do so in a balanced and measured manner
- think before responding to comments and, when in doubt, get a second opinion
- seek advice and report any mistakes using the school’s reporting process
- consider turning off tagging people in images where possible

The Don’ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- don’t publish confidential or commercially sensitive material
- don’t breach copyright, data protection or other relevant legislation
- consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- don’t use social media to air internal grievances

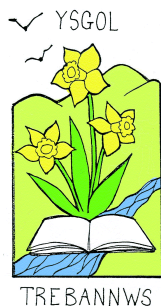
C1 Responding to incidents of misuse – flow chart



C2 Reporting Log Template

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		



Ysgol Gynradd Gymraeg Trebannws Trebannws Welsh Primary School

Pennaeth/Headteacher: Mrs R.Evans



C3 Record of reviewing devices/internet sites

(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

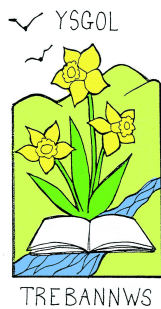
Name and location of computer used for review (for web sites)

--

Web site(s) address/device

Reason for concern

Conclusion and action proposed or taken



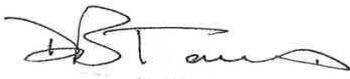
Ysgol Gynradd Gymraeg Trebannws Trebannws Welsh Primary School



C4 Training Needs Audit Log Template

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date		

Designation / Name	Signature	Date
Chair of Governors		7/6/17
Headteacher		

Review Date	May 2018
------------------------	----------