Ysgol Aberconwy

E-Safety Policy

POLICY DOCUMENT NO: 80	**ISSUE NO: 1**

THIS POLICY HAS BEEN APPROVED BY THE FULL GOVERNING BODY

Signed:

Date: 11/03/25

Review due date : 01/03/27 **LT Link : KB**

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

Contents

Introduction

Purpose of the e-Safety Policy

The school e-Safety Policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding, Behaviour and Anti-Bullying policies.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their e-Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

The policy statements herein are, in the view of Welsh Government, essential in any school e-Safety Policy, based on good practice.

An effective school e-Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the school community.

It is suggested that consultation in the production of this policy should involve:

- Governors
- Teaching Staff and Support Staff

Due to the ever changing nature of digital technologies, it is best practice that the school reviews the e-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place.

Development / Monitoring / Review of this Policy

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

- Headteacher / Senior Leaders
- e-Safety Officer
- Staff – including Teachers, Support Staff, Technical staff
- Governors

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

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	
The implementation of this e-Safety policy will be monitored by the:	*Business Manager*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	*Annually*
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police, Parents*

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*
  - *staff*

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals[1] and groups within the school :

1. Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governing body* receiving periodic information about significant e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor to include:

- *meeting with the e-Safety Officer*
- *reporting to relevant Governors meetings*

In addition, Governors who access school systems / website / Intranet as part of the wider school provision will be expected to sign a Governor User AUA before being provided with access to school systems.

2. Headteacher 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 Officer*.
- The Headteacher and (at least) another member of the Senior Leadership 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.
- *The Headteacher is responsible for ensuring that the e-Safety Coordinator Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.*
- *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.*

3. e-Safety Officer:

The *e-Safety 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 incidents
- attends relevant meeting of Governors
- reports significant issues periodically to Senior Leadership Team

4. Network Manager / Technical staff:

NOTE: 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 technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety policy and procedures.

The *Technical Staff* are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) 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 (if one exists), is applied and updated on a regular basis
- 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, Senior Leadership Team; e-Safety Officer for investigation / action / sanction as appropriate
- that monitoring software / systems are implemented and updated as new updates are released

5. 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 (AUP / AUA)
- they report any suspected misuse or problem to the Headteacher / e-Safety 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
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-Safety and acceptable use agreements
- 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 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

6. Safeguarding Designated Person

NOTE: It is important to emphasise that these are safeguarding **issues**, not technical issues; the technology provides additional means for safeguarding issues to develop.

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

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

7. e-Safety Group

Having an 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.

Members of an e-Safety Group would assist the e-Safety Officer with:

- the production / review / monitoring of the school e-Safety policy / documents.
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- 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)

8. Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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

9. 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 assist parents to understand these issues through parents' evenings, newsletters, letters, website / Intranet 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
- their children's personal devices in the school (where this is allowed)

Policy Statements

1. Pupils

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

e-Safety 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 / Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the 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 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

2. 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
- Parents / Carers evenings / sessions
- High profile events / campaigns eg. Safer Internet Day

3. Governors

The school will provide opportunities for Governors to gain from the school's e-Safety knowledge and experience. This may be offered through the following:

- Providing learning courses in use of new digital technologies, digital literacy and e-Safety
- Targeted e-Safety messaging
- Intranet / website will provide e-Safety information for the wider community

4. 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.
- 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 Officer 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 Officer will provide advice / guidance / training to individuals as required.

5. Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in 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

6. Technical – infrastructure / equipment, filtering and monitoring

The school has an IT engineer and IT Manager supplemented by IT support from various 3rd parties for both hardware and software.

The school will also check Local Authority / other relevant body policies on these technical issues.

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 as laid out by Conwy CBC and Welsh Government
- 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 will be provided with a username and secure password by the IT engineer / Head of ICT department and IT Manager who collectively will keep an up to date record of users and their usernames in their respective areas. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the IT engineer must also be available to the IT Manager/Business Manager and kept securely.
- The IT Manager 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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.
- The school has enhanced / differentiated user-level filtering allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc)
- The IT engineer and IT Manager regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- A system of alerts from the filtering and firewall software is in place for monitoring and reporting any actual / potential technical incident / security breach to the IT engineer / IT Manager
- Security measures are in place to monitor and 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 for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems via the IT engineer and IT Manager.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- Removal media is blocked on school devices to ensure the school network is protected from malicious software. (eg memory sticks / CDs / DVDs)

7. Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded on 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 utilising 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. The school is bringing that familiar digital life into the school classroom by providing a variety of school owned devices as well as allowing pupils in the 6th Form to use their own laptops/tablets/Mac books and chromebooks. 6th Form pupils are added to a BYOD group that applies the same filters as when using a school device.
Pupils in the 6th Form 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.
Pupils in KS3/4 are not allowed to use their own devices on the school site unless permission is provided by a member of staff.

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.

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 polices 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.

In the school, there are clear rules as to when mobile devices can be used during lessons:

- Mobile devices are not permitted during this lesson;
- Mobile devices can be used during this lesson but they must stay in learner's bag until the teacher allows their use; and
- Mobile devices can be brought out and placed on the desk.

8. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites.
- 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.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

9. 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 on website)
- It has a Data Protection Policy (see policy on Intranet)
- 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/or secure password protected devices.

Removal media devices are blocked by the school.

10. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages (6th Form have additional privileges):

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x				X			
Use of mobile phones in lessons		x					x	
Use of mobile phones in social time		x				6th		x
Taking photos on mobile phones / cameras		x					6th	x
Use of other mobile devices eg tablets, gaming devices		x				6th	x	
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of messaging apps		x				6th		x
Use of social media		x				6th		x
Use of blogs		x				6th		x

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 pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg 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 pupils or parents / carers (email, chat, Intranet 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.
- Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11. Social Media - Protecting Professional Identity

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 pupils, 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 puts them in a position of trust and that their conduct should reflect this.

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

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

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

School staff should ensure that:

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

The school's use of social media for professional purposes will be checked regularly by the e-safety Officer to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

12. Unsuitable / inappropriate activities

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

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

User Actions :		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, 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	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				x		
On-line gaming (non educational)					x	
On-line gambling					x	
On-line shopping / commerce		x				
File sharing		x				
Use of social media			x			

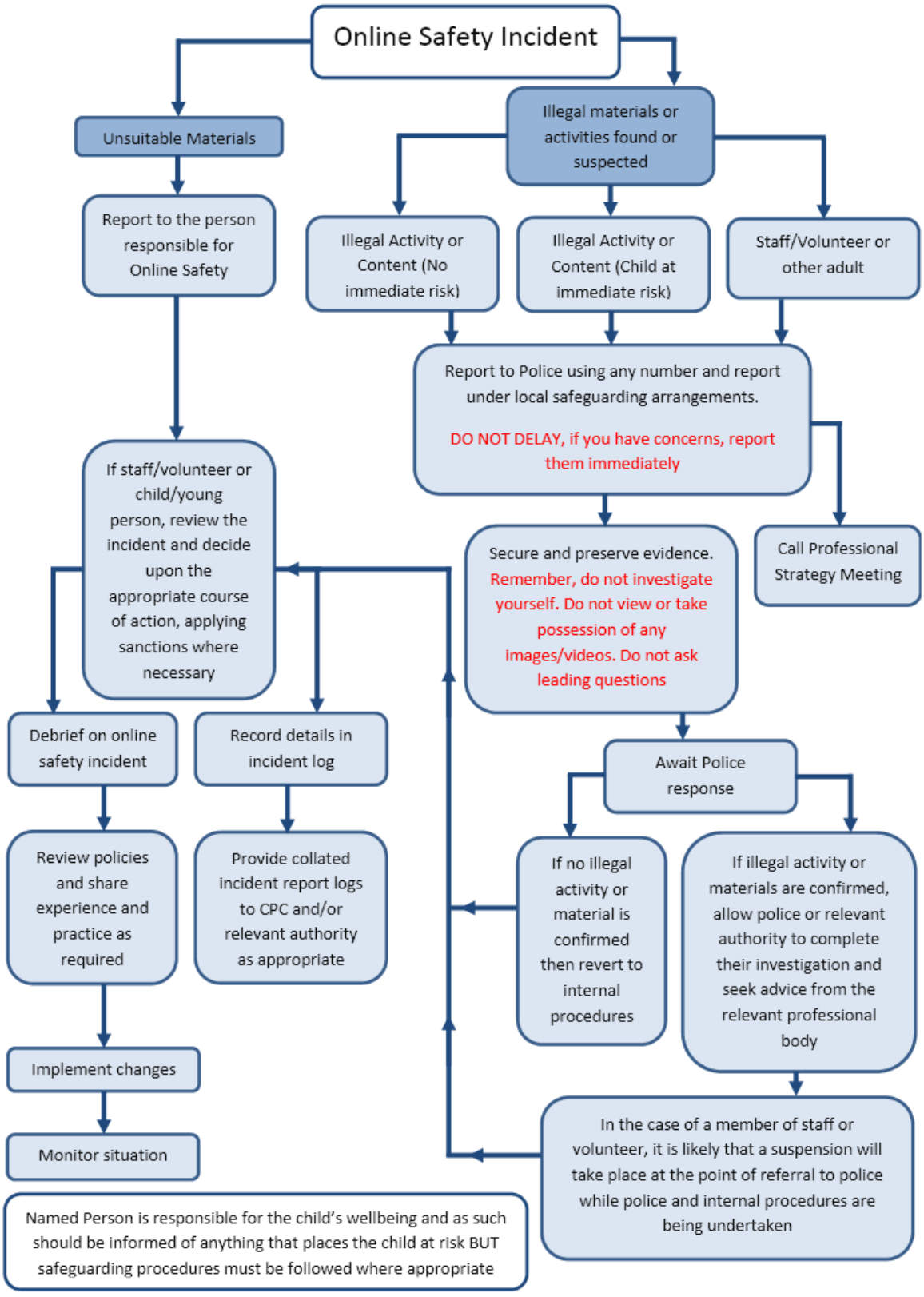
Use of messaging apps		x			
Use of video broadcasting eg Youtube			x		

13. 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.

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) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils Actions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another student's / pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff Actions

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

Appendix 1 : Additional Documentation

Copies of further detailed templates can be downloaded from https://hwb.wales.gov.uk

Acceptable Use Agreements

- A1 Student / Pupil Acceptable Use Agreement template (younger children)
- A2 Student / Pupil Acceptable Use Agreement template (older children)
- A3 Staff and Volunteers Acceptable Use Agreement template
- A4 Parents / Carers Acceptable Use Agreement template
- A5 Community Users Acceptable Use Agreement template

Specific Policies

- B1 School Technical Security Policy template
- B2 School Personal Data Policy template
- B3 School Bring Your Own Devices (BYOD) Template Policy
- B4 School e-Safety Committee Terms of Reference

Support documents and links

- C1 Responding to incidents of misuse – flowchart
- C2 Record of reviewing sites (for internet misuse)
- C3 School Reporting Log template
- C4 School Training Needs Audit template
- C5 Summary of Legislation
- C6 Office 365 – further details
- C7 Links to other organisations and documents

Acknowledgements

WG and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School e-Safety Policy Template and of the 360 degree safe e-Safety Self Review Tool:

- Members of the SWGfL e-Safety Group
- Representatives of SW Local Authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendix 2 : Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-Safety policy.

UK Safer Internet Centre

- Safer Internet Centre
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - http://www.netsmartz.org/index.aspx

Support for Schools

- Specialist help and support - SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour
- Welsh Government – Respecting Others
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

- Digizen – Social Networking
- SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- SWGfL Digital Literacy & Citizenship curriculum
- Alberta, Canada - digital citizenship policy development guide.pdf
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Somerset - e-Sense materials for schools

Mobile Devices / BYOD

- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN - Guidance Note - BYOD

Data Protection

- Information Commissioners Office:
  - Your rights to your information – Resources for Schools - ICO
  - ICO pages for young people
  - Guide to Data Protection Act - Information Commissioners Office
  - Guide to the Freedom of Information Act - Information Commissioners Office
  - ICO guidance on the Freedom of Information Model Publication Scheme
  - ICO Freedom of Information Model Publication Scheme Template for schools (England)
  - ICO - Guidance we gave to schools - September 2012 (England)
  - ICO Guidance on Bring Your Own Device
  - ICO Guidance on Cloud Hosted Services
  - Information Commissioners Office good practice note on taking photos in schools
  - ICO Guidance Data Protection Practical Guide to IT Security
  - ICO – Think Privacy Toolkit
  - ICO – Personal Information Online – Code of Practice
  - ICO – Access Aware Toolkit
  - ICO Subject Access Code of Practice
  - ICO – Guidance on Data Security Breach Management
- SWGfL - Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- Somerset - Flowchart on Storage of Personal Data
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Kent - Safer Practice with Technology
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Note - esecurity SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

Working with parents and carers

- SWGfL BOOST Presentations - parents presentation
- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- DirectGov - Internet Safety for parents

- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops / education
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- The Cybersmile Foundation (cyberbullying) - advice for parents

Research

- EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
- Futurelab - "Digital participation - its not chalk and talk any more!"

Appendix 3 : Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-Safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol