Milford Haven School
Networking e-Safety
Policy (*Oct 2017*)

….…………………..…………. …………………………… (Signed by Chair)

…………………………………………………………………..*Date*

This policy will be reviewed on or before the following date ………………….

MILFORD HAVEN SCHOOL

e-Safety Policy

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:

- *Senior Leaders*
- *e-Safety Officer*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*
- *Community users*

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

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the Governing Body / Governors Sub Committee *on:*	*11/10/2017*
The implementation of this e-Safety policy will be monitored by the:	*e-safety working group*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	*Annually at Full Governors Meeting – Autumn to review previous year*
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:	*Summer Term 2018*
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*LA Child Care Assessment Team (CCATs), Police: SCPO and Police Liaison Officer.*

The school will monitor the impact of the policy using:

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

If possible – may need the assistance of service provider

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Pastoral, Personnel and Curriculum 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 Governor to include:

- regular meetings with the e-Safety 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 and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community, although the day to day responsibility for e-Safety may be delegated to the e-Safety Officer (EK).

- 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.[1]

- The Headteacher/Senior Leaders are responsible for ensuring that the e-Safety 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/Senior Leaders 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 will receive regular monitoring reports from the e-Safety Officer.

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 and creates a log of incidents to inform future e-Safety developments.
- meets regularly with e-Safety Link 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

---

[1] as referenced in the Staff (and Volunteer) ICT Acceptable Use Policy Agreement

 see flow chart on dealing with e-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures.

Network Manager / Technical staff:

The Network Support 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 Technical Security Policy (which does not currently exist in MHS), 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 / Senior Leader; e-Safety Officer / Heads of Years / Pastoral Officers / Leaders of Learning 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 (AUP).
- they report any suspected misuse or problem to the 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 i.e. Google accounts.
- Use of personal devices is in line with the Staff AUP.
- 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 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 including own devices 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 processes are in place for dealing with any unsuitable material that is found in internet searches.

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 or those with Tier 2 Child Protection Training should be trained in 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

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. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the e-Safety 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.

A Milford Haven School e-Safety Group Terms of Reference can be found in the appendices.

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 parents' evenings, 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 by Network Support Staff. A copy of the AUA should be kept securely in the Network Office.

Policy Statements

Education – young people

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 PSE 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.
- it is accepted that from time to time, for good educational reasons, pupils 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 Network Support Staff 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:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / 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 (see school website for further links / resources)

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:

- Providing family learning courses in use of new digital technologies, digital literacy and e-Safety.
- 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.
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-Safety provision.

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 programme of 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 Officer or nominated person will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be made available to staff and comments welcomed.
- The e-Safety Officer or 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 subcommittee / 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.

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 (these may be outlined in Local Authority / other relevant body policy and guidance).
- 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 Network Support who will keep an up to date record of users and their usernames. Users are responsible for the security of

their username and password and will be required to change their password every 45 days for staff and sixth form students. Pupils in KS3 and KS4 passwords will be changed at the start of an academic year.

- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated person and kept in a secure place (eg school safe)
- The Business 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.
- 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 via the school ticketing system (mhshelp).
- Network Support Staff will configure systems to provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc).
- Where possible, school technical staff 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.
- An appropriate procedure is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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. All "guests" will be required to agree and sign the Staff (and Guest) Acceptable Use Agreement.
- The Staff (and Guest) AUA has a section regarding the extent of personal use that users (staff / students / pupils / community users) and other third-parties are allowed on school devices that may be used out of school.
- Network rules that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- The Staff (and Guest) AUA has a section 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.

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 utilising the school's wireless network. The device then has access to the wider internet including the school's e- 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 (template policy statements are found below) 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 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. Staff need to reinforce the agreed rules and sanctions using the Traffic Light display material in their teaching area.

Practical rules should mobile devices be brought out and placed on the desk include:

- Screens must be visible at all times i.e. face up on the desk
- In the event of a safeguarding concern, student devices may need to be viewed by the eSafety Officer or other nominated person
- Photographs and videos cannot be taken without the authorisation of the teacher
- Breaches of the trust being given to the students must be dealt with according to the consequences and sanctions identified in the Milford Haven School Positive Behaviour Policy.

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 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 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). These images should not contain

any children other than their own. 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 (Using Images of Children Policy) concerning the sharing, distribution and publication of those images. These 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- 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 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.

Data Protection

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

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

The school must ensure that:

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

- Take all reasonable precautions when transferring data and should ensure they are using encryption and secure password protected devices.

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow pupils 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 pupils. 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:

Communication Technologies	Staff & other adults				Students / Pupils			
	A	CT	SS	NA	A	CT	SP	NA
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							X
Taking photos of others on mobile phones / cameras				X				X
Taking photos of work on mobile phones / cameras				X			X	
Use of other mobile devices eg tablets, gaming devices	X						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					X	
Use of social media		X					X	
Use of blogs	X				X			

A = Allowed
CT = Allowed at certain times
SS = Allowed for selected staff
SP = Allowed with staff permission
NA = Not allowed

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 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, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

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

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

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

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:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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				

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.
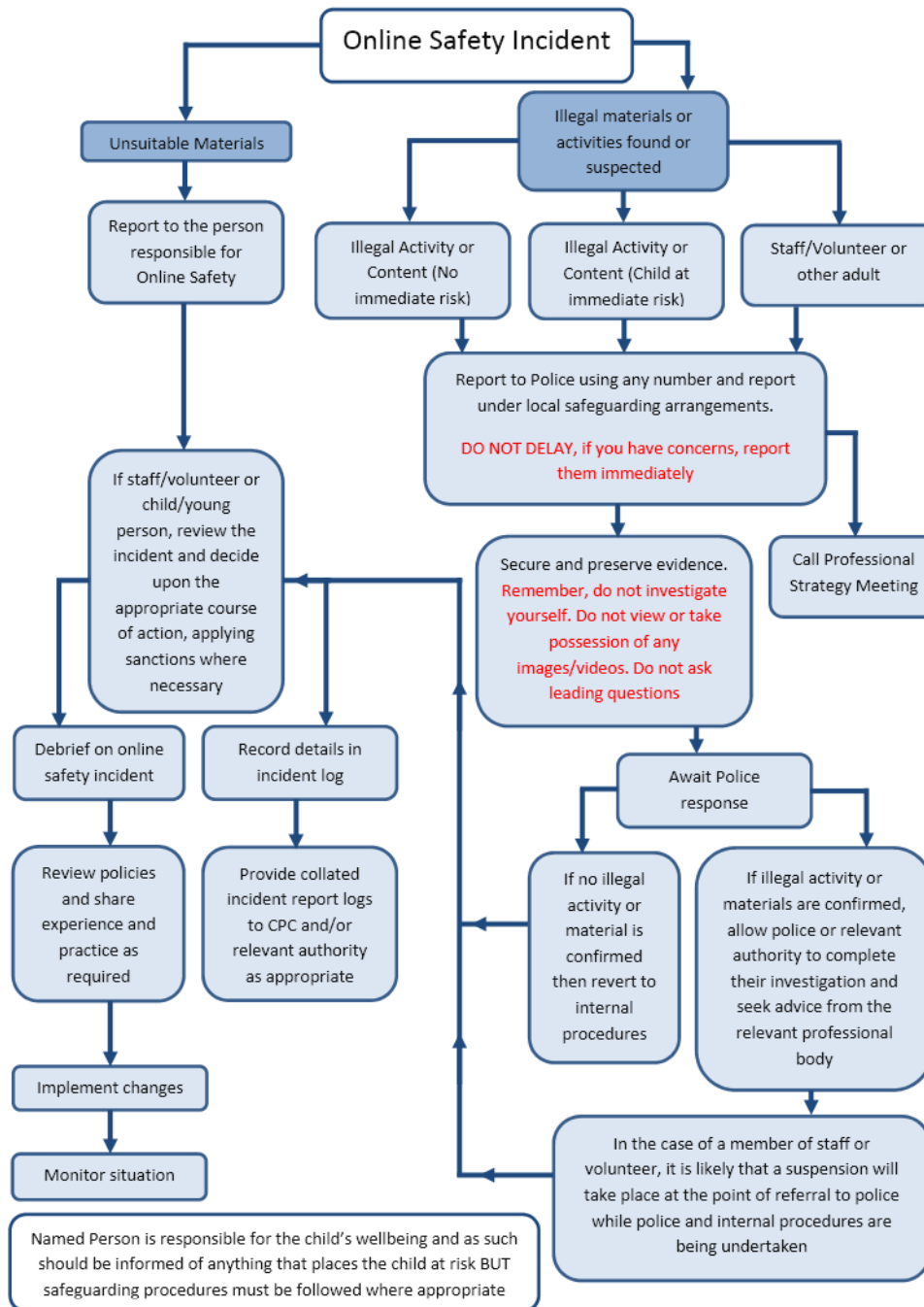
Other Incidents

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.

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 LoL / HoY / On Call / other	Refer to Head teacher / Duty SLT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of 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		X	X		X
Unauthorised use of non-educational sites during lessons	X								X
Unauthorised use of mobile phone / digital camera / other mobile device	X								X
Unauthorised use of social media / messaging apps / personal email	X	X							X
Unauthorised downloading or uploading of files	X							X	
Allowing others to access school network by sharing username and passwords		X			X		X		
Attempting to access or accessing the school network, using another student's / pupil's account		X			X		X		
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X	X	X		X
Corrupting or destroying the data of other users		X	X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X	X	X		X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X	X	X		X
Using proxy sites or other means to subvert the school's filtering system		X			X				
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X		X	X	X		X

Staff   Actions

Incidents:	Refer to line manager	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			X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
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	X	X			X	X		X
Careless use of personal data eg holding or transferring data in an insecure manner		X			X	X		
Deliberate actions to breach data protection or network security rules		X			X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X			X	X	X	X
Actions which could compromise the staff member's professional standing	X	X			X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X	X	X
Using proxy sites or other means to subvert the school's 's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X		X	X

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