YSGOL WIRFODDOL EGLWYSIG Y MODEL
MODEL CHURCH IN WALES SCHOOL

Mission Statement

The Model Church in Wales School's mission is to work within a Christian ethos to nurture and develop all that is best in our pupils providing them with a sure foundation for their future.

E-Safety Policy

Policy confirmed by the Governing body of Model Church in Wales School on:

Date: ……

Signed: …… (Chair of Governors)

…….. (Headteacher).

Reviewed Date: 8/2/18 – Panel: Policy]

"Jesus our 'Model',
Helps us to share
Learning and Kindness,
Friendship and care"

Development / Monitoring / Review of this Policy

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

- *Headteacher/ e-Safety Officer – Mrs Amanda Bowen-Price*
- *ICT Co-ordinators – Foundation Phase – Mrs Sarah Hart / Key Stage 2 – Miss Lisa England*
- *Staff representations – Mrs Mari Hughes (deputy head) / Mrs Kimberly Good / Mrs Gail Hawkins / Mrs Rachael Evans*
- *E-Safety Governor – Mr Mike Kirby*

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*Autumn 2015*
The implementation of this e-Safety policy will be monitored by the:	*E-Safety Committee*
Monitoring will take place at regular intervals:	*Every year*
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:	*Every 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.	
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LA ICT Manager, , Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-Safety Governor. The role of the e-Safety Governor will include:

- *regular meetings with the e-Safety Committee*
- *regular monitoring of e-Safety incident logs*
- *reporting to relevant Governors*

Headteacher / Principal and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community**.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents included in a later section).**
- *The Headteacher / Senior Leaders are responsible for ensuring that 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.*

e-Safety Coordinator / Officer:

The *e-Safety Coordinator / Officer*

- liaises closely with 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
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- meets regularly with e-Safety *Governor* to discuss current issues
- reports regularly to Senior Leadership Team

Managed Service Provider (County)

The *M*anaged service provider is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets the required e-Safety technical requirements as identified and any local authority e-Safety guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection procedure, in which passwords are regularly changed**

- ***that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person***
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher* for investigation / action / sanction
- *that monitoring 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 schoole-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* 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 / policies***
- **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 etcin lessons and other school activities (where allowed) and implement current policies with regard to these devices**
- **in lessons where internet use is pre-plannedpupils 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***

Child Protection / Safeguarding Designated Person

The *Safeguarding Designated Person*should be trained in e-Safety issues and be aware of the potential for serioussafeguarding 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.

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

- the production / review / monitoring of the school e-Safety policy
- 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

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement**
- Key Stage 2 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'se-Safety Policy covers their actions out of school, if related to their membership of the school
- should be able to tell a responsible adult if anything is upsetting them on the internet

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, website, information about national / local e-Safety campaigns. 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
- their children's personal devices in the school

Volunteers / Community Users

Volunteers / Community Users who access school systems / website as part of the wider school provision will be expected to sign a Volunteer User AUA before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education 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 / PSD / Digital Literacy lessons or other lessons and should be regularly revisited**
- **Key e-Safety messages should be reinforced as part of a series of assemblies**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (Key Stage 2)**
- *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 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.*

Education – parents / carers

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

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

- ***Letters, newsletters, web site,***
- ***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**

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. (January 2016)**
- **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 ICT Coordinators will receive regular updates through attendance at external training events***
- ***This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.***

Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub committee. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation (egSWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **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
- *An appropriate system is in placefor users to report any actual / potential technical incident / security breach*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- *An agreement is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school.*
- *Staff have to sign out any equipment which is leaving school premises.*
- *Staff are forbidden from downloading executable files and installing programmes on school devices, unless permission is granted.*
- *Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

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 andpupils 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 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 unless consent is sought from parents.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website*

Data Protection

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

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

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.**
- **It has a Data Protection Policy.**
- Risk assessments are carried out when required.
- 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 are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

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

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

Communications

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

	Staff and other adults in school				Pupils			
Communications	Allowed	Allowed at certain times (e.g. lunchtime)	Allowed for certain staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought into school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones				✓				✓
Use of other personal mobile devices		✓						✓
Use of personal email addresses in school/on school network		✓						✓
Use of school email for personal email				✓				✓
Use of messaging apps **(on personal mobile phone or device only)**		✓						✓
Use of social media **(on personal mobile phone or device only)**		✓						✓
Use of personal blogs **(on personal mobile phone or device only)**		✓						✓

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*
- 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.*
- *Whole class / group email addresses may be used at KS1, whilepupils at KS2 will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-Safety issues, such as the risks attached to thesharing 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.*

In instances where devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the

user and their parents/carers as does the liability for any loss or damage resulting from the use of the device in school.The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school.

The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network.

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 Education Workforce Council (EWC) 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 (see Appendix for *Guide to using social media responsibly*)
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

In relation to personal social media account school staff should ensure that:

- They make no reference 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 committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate 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

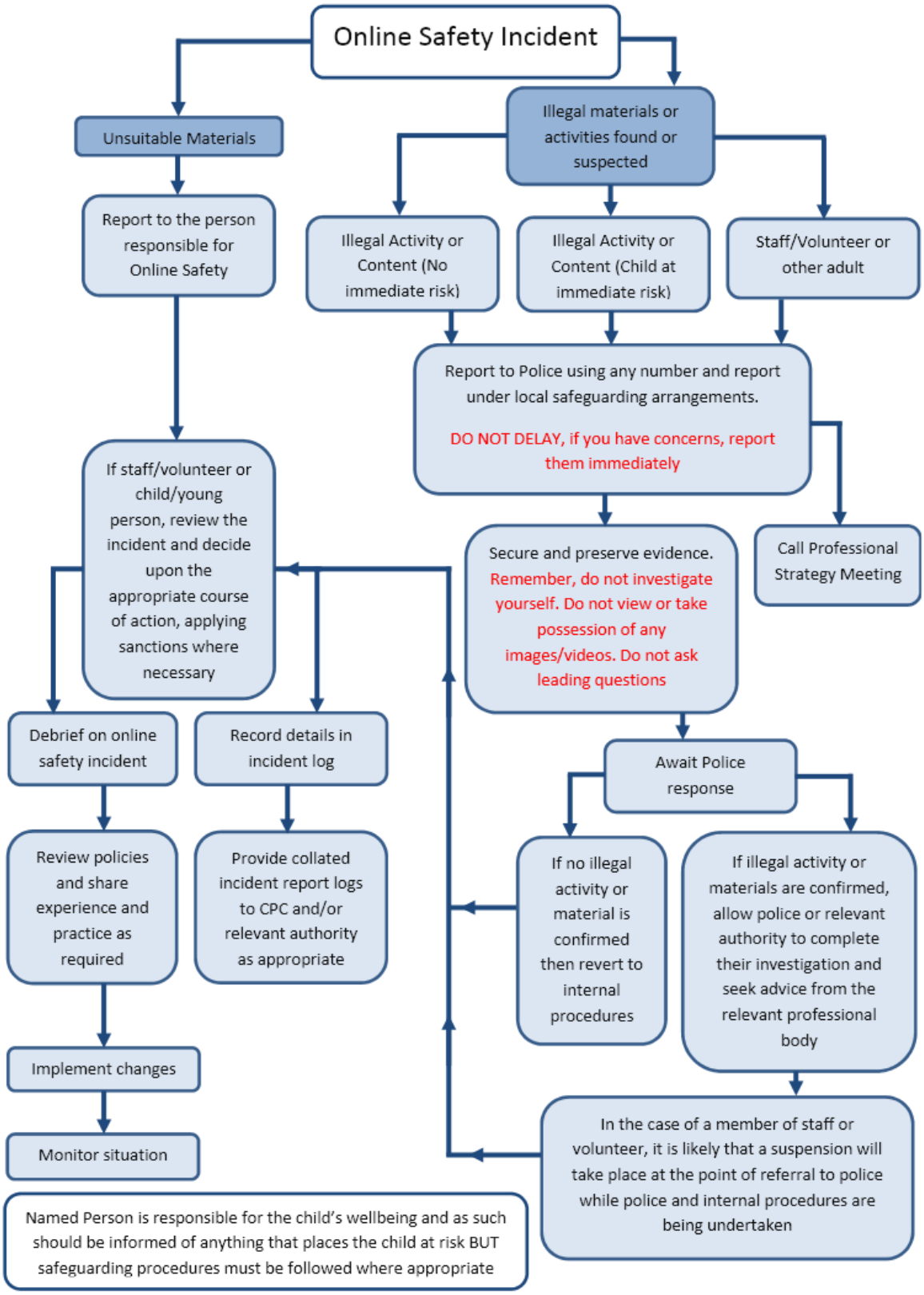
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	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					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
On-line gaming (educational)			✓			
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping / commerce					✓	
File sharing					✓	
Use of social media				✓		
Use of messaging apps			✓			
Use of video broadcasting egYoutube					✓	

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 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 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 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 abusethen 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.

Actions and Sanctions
Pupils

Incidents:	Refer to class teacher to ensure they are aware	Refer to ICT/E-safety co-ordinator	Refer to Headteacher	Refer to Police	Refer to county	Inform parents / carers	Removal of network / internet access rights	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
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 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 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

Incidents:	Refer to line manager to ensure they are aware	Refer to ICT/E-safety Coordinator	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	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).	✓	✓	✓	✓	✓		✓	✓
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 e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓			✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓			✓	✓
Sending an email, text or 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 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 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		✓	✓	✓	✓		✓	✓

Appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

https://hwb.wales.gov.uk

1. Student acceptable use agreement
2. Staff & Volunteer acceptable use agreement
3. Record of reviewing devices/internet sites (responding to misuse)
4. Termly log of incidents
5. EWC – Guide to using social media responsibly
6. ERW – Dealing with adverse comments and complaints against schools on social media

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 SWGfLe-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

Summary of Legislation

Schools should be aware of the legislative framework under which this e-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Criminal Justice & Public Order Act 1994 / Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006 / Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education
- The right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems