



CYNGOR CAERDYDD  
CARDIFF COUNCIL

## Western Learning Federation Ty Gwyn School



### E-Safety Policy

Date Reviewed:	1 <sup>st</sup> July 2021
Date for Review:	1 <sup>st</sup> July 2023
Date Published:	February 2022
Ratified by Governors:	14 <sup>th</sup> July 2021

**MONITORING THE POLICY**

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

Signed: ..... *W.A.M.* ..... Date: ..... *1/12/21* .....  
Executive Headteacher

Signed: ..... *D. Shea* ..... Date: ..... *8/11/21* .....  
Head of School

Signed: ..... *J. Saunders* ..... Date: ..... *8.11.21* .....  
Chair of Governors



# The Western Learning Federation

## Our Vision, Mission Statement, Values & Principles

### Our Vision

Together we learn, grow and achieve





### Our Mission Statement

Together we collaborate in all that we do

### Our Values and Principles



Our vision and values have been developed using the UN Convention on the Rights of the Child (UNCRC) as our guide, to create a safe and inspiring place to learn, where children are respected, their talents are nurtured and they are able to thrive. Our vision and values also compliment the 'Four Purposes of Learning' which underpin Curriculum for Wales. The Four Purposes are the shared vision and aspiration for every child and young person in Wales and support our pupils to become; Ambitious Capable Learners Healthy Confident Individuals Enterprising Creative Contributors Ethical Informed Citizens.

<b>Ambitious Capable Learners</b> 	<b>Healthy Confident Individuals</b> 	<b>Enterprising Creative Contributors</b> 	<b>Ethical Informed Citizens</b> 
--	---	--	---

## 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 Technology Group (including e-Safety Governor) 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 Co-ordinator
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant governors / governing body

### Headteacher and Senior Leaders:

- The *Headteacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety is delegated to the *e-Safety Co-ordinator*.
- The Headteacher and 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.
- Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator.

### e-Safety Coordinator:

The *e-Safety Coordinator*:

- leads the e-Safety committee (Technology Group)
- 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 *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

### Technical staff:

Technical Staff (or managed service provider) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets (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 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 e-Safety Coordinator / Senior Leadership Team

## 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 Agreement ( AUA)
- they report any suspected misuse or problem to the *Senior Leadership Team / e-Safety Coordinator / Technology Group* 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
- students / pupils understand and follow the e-Safety and acceptable use *agreements / policies*
- students / pupils have the understanding appropriate to their level of additional learning need (ALN) of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use

## Safeguarding Designated Person

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

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

## e-Safety Group (part of Technology Group)

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

Members of the e-Safety Group (or other relevant group) will assist the e-Safety Coordinator with:

- the production / review / monitoring of the school e-Safety policy / documents.
- *the production / review / monitoring of the school filtering arrangement 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

## **Students / pupils:**

The pupils at Ty Gwyn all have Additional Learning Needs (ALN) with the vast majority having either Profound and Multiple Learning Difficulties (PMLD) or Severe Learning Difficulties (SLD). Therefore the expectations below do not apply to our pupils however they are useful aspirational targets.

- 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.

# Policy Statements

## Education – young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of 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 Digital Competence Framework (DCF) includes e-safety which is embedded throughout the curriculum as part of the cross curricular area of digital competence. 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 adapted to the level of the pupils should be provided which is embedded in the contexts for learning and should be regularly revisited
- Key e-Safety messages (appropriate to the level of the pupils) should be reinforced as part of a planned programme of assemblies / activities
- Where appropriate 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.
- Where appropriate pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – parents / carers

Many parents and carers have do not have a full 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

## 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 website will provide e-Safety information for the wider community

## **Education & Training – Staff / Volunteers**

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

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.
- The e-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinator will provide advice / guidance / training to individuals as required.

## **Training – Governors**

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- 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.
- All staff users will be provided with a username and secure password. Users are responsible for the security of their username and password
- Pupils use group class log-ons and passwords unless the Technology Group deems that it is appropriate for a pupil to have an individual username
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (Cardiff Schools IT) must also be available to the Headteacher or other nominated senior leader
- The e-Safety Co-ordinator and Technology Group are 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
- Internet access is filtered for all users.
- 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.

## **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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 in ways appropriate to their ability 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

## **Data Protection (Please also refer to data protection policy)**

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

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must 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:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones / personal cameras								
Use of other mobile devices eg tablets, gaming devices								

Use of personal email addresses in school, or on school network		Yellow						Red
Use of school email for personal emails				Red				Red
Use of messaging apps		Yellow					Orange	
Use of social media		Yellow					Orange	
Use of blogs		Yellow					Orange	

When using communication technologies the Ty Gwyn Special School considers the following as good practice:

- The official school email service (Cardiff.gov and Hwb mail) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the e-Safety Co-ordinator / Senior Leadership Team / Technology Group in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils should be taught about e-Safety issues in ways which are appropriate to their ability, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

## Social Media - Protecting Professional Identity

Expectations for teachers' and teaching assistants 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 staff members are aware of and have copies of the EWC Code of Professional Conduct and Guide to using social media responsibly.

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

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

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

School staff should ensure that:

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

The school's use of social media for professional purposes will be checked regularly by the e-Safety Co-ordinator / Technology Group 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. Ty Gwyn 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
<b>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:</b>	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 for responding to online safety incidents and report immediately to the police.**

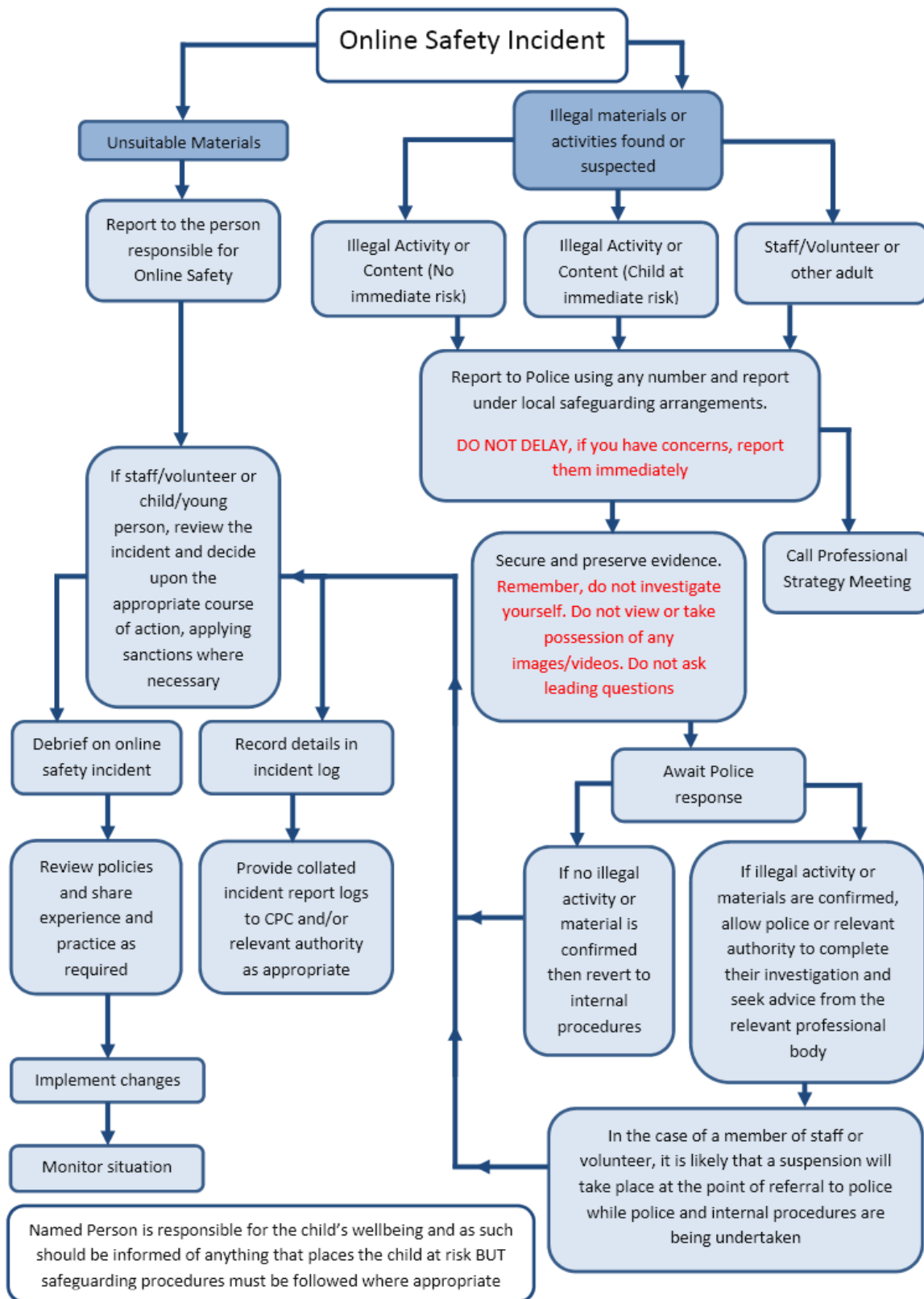
### Prevent

The UK faces a range of terrorist threats. All the terrorist groups who pose a threat seek to radicalise and recruit people to their cause. But the percentage of people who are prepared to support violent extremism in this country is very small. It is significantly greater amongst young people.

We now have more information about the factors which encourage people to support terrorism and then to engage in terrorist-related activity. It is important to understand these factors if we are to prevent radicalisation and minimise the risks it poses to our national security. We judge that radicalisation is driven by an ideology which sanctions the use of violence; by propagandists for that ideology here and overseas; and by personal vulnerabilities and specific local factors which, for a range of reasons, make that ideology seem both attractive and compelling. There is evidence to indicate that support for terrorism is associated with rejection of a cohesive, integrated, multi-faith society and of parliamentary democracy. Work to deal with radicalisation will depend on developing a sense of belonging to this country and support for our core values. Terrorist groups can take up and exploit ideas which have been developed and sometimes popularised by extremist organisations which operate legally in this country.

Prevent training has been delivered to the whole school staff and regular updates are shared in the whole school daily briefing. As much of the potential radicalisation and recruitment activities take place online this is a particular e-Safety concern as well as a wider safeguarding issue. Inappropriate or Illegal material which is seeking to radicalise and / or recruit pupils / staff / stakeholders should be treated as an online safety incident and should always be reported to a member of the senior leadership team. Due to the nature of

their learning difficulties it would not be possible for the vast majority of the pupils at Ty Gwyn Special School to engage radicalisation activities; however it remains possible that an incident could occur.



## Other Incidents

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

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

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

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

## School Actions

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

Due to the nature of their learning difficulties it would not be possible for the vast majority of the pupils at Ty Gwyn Special School to engage in any of the activities listed in the table below; however it remains possible that an incident could occur. It is appropriate that each incident is judged on an individual basis therefore the table below does not show a correlation between incident and action but is useful for highlighting possible incidents and the potential actions.



## Students / Pupils

## Actions

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

## Staff

## Actions

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

## Acknowledgements

Ty Gwyn School acknowledges Welsh Government (WG) and South West Grid for Learning (SWGfL) for providing the template on which this policy is based.

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

Copyright of these Template Policies is held by SWGfL. Schools and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([esafety@swgfl.org.uk](mailto:esafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2014. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2014