Dinas Powys Primary 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.

Contents

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 Governing body receiving information about e-Safety incidents and monitoring reports. A member of the Governing Body will take on the role of e-Safety / Safeguarding Governor.

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 Deputies should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the e-Safety Coordinators (both sites) 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.

e-Safety Coordinator (both sites):

The e-Safety Coordinator

- 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 advice for staff
- liaises with the Local Authority
- 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

Technical staff:

The Vale of Glamorgan Technician Service is responsible for ensuring:

- that Dinas Powys Primary 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.

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 Headteacher / e-Safety Coordinator / Safeguarding Officer for investigation / action
- all digital communications with students / pupils / parents / carers is on a professional level
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- they ensure that pupils understand and follow the e-Safety and acceptable use policy
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that 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 Safeguarding Officer 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.

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

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

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- should understand the importance of adopting good e-Safety practice when using digital technologies out of 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 the website and other relevant literature and/or information sessions. 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 Hwb+

Community Users

Community Users (e.g Playworks After School Club) who access school systems 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 pupils to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and circle time activities
- Older 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, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Vale of Glamorgan Filtering Service 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

- The School Website
- High profile events / campaigns eg Safer Internet Day
- Relevant literature

Education – The Wider Community

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.
- 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 Coordinators will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET as appropriate.
- The e-Safety Coordinators will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in relevant e-Safety training / awareness sessions as appropriate, e.g.

- 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

- 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.
- Software licence logs must be accurate and up to date. Regular checks should be made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- An appropriate system 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, 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. 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). 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 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website as part of the AUA signed by parents or carers on entry to school.

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 will ensure that:

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

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.
- 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 students / pupils or parents / carers must be professional in tone and content.
- Pupils, particularly pupils at KS2, may be provided with Hwb+ email addresses for educational use
- Pupils will 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.

Social Media - Protecting Professional Identity

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.

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 senior risk officer and 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,	**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

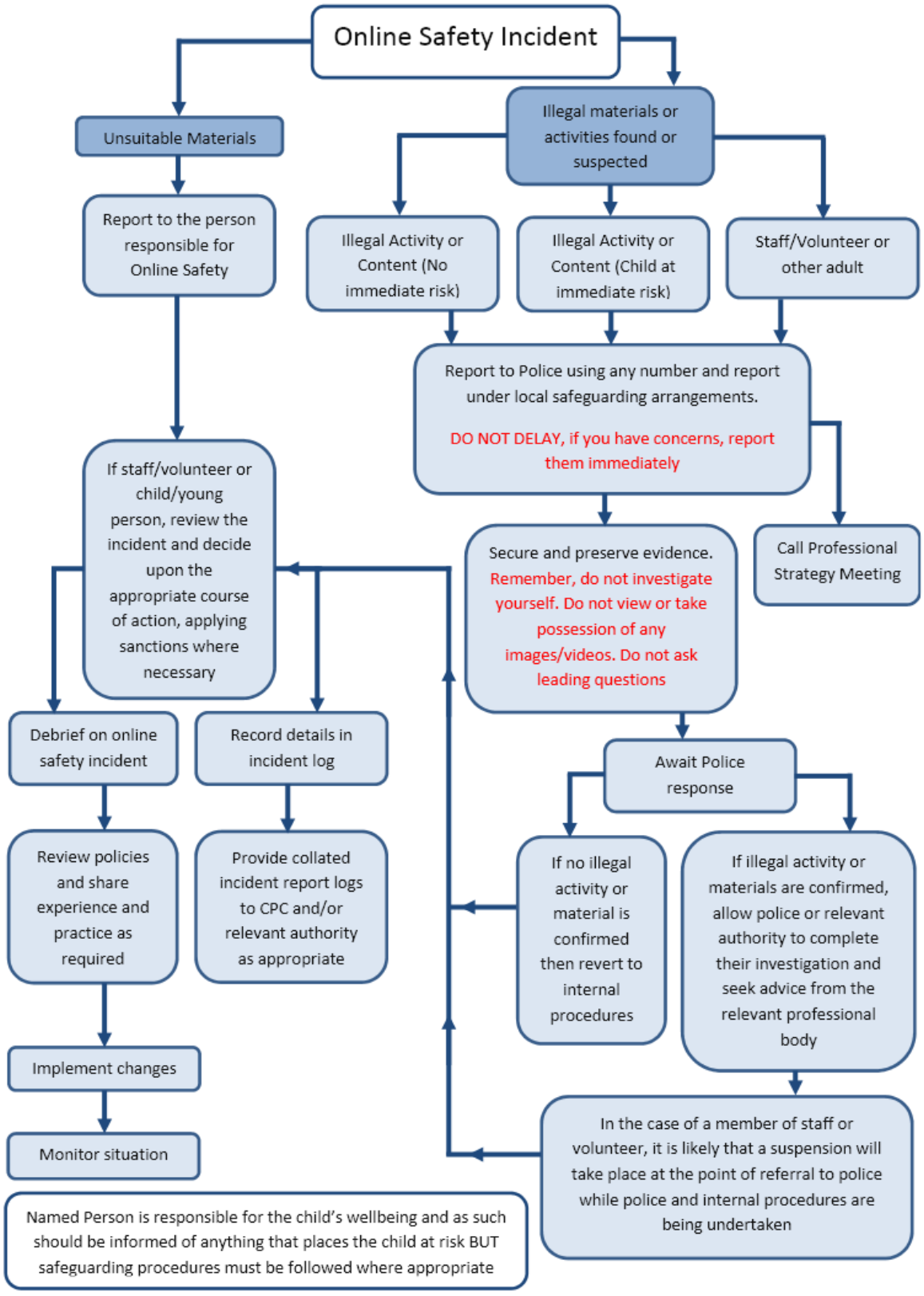
post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008**					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.

School Actions

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

Students / Pupils Actions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X		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	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						
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		X	X					
Continued infringements of the above, following previous warnings or sanctions			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		
Using proxy sites or other means to subvert the school's 's filtering system					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		
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 line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	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		
Careless use of personal data eg holding or transferring data in an insecure manner		X				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	X	X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					
Using proxy sites or other means to subvert the school's 's filtering system		X	X	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	X
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X				X	X	X

Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by Dinas Powys Primary School e-Safety Group made up of:

- Headteacher / Senior Leaders
- e-Safety Coordinator (both sites)
- ICT Technician
- E-Safety Governor
- Parent Representative
- Pupil Representative
- Support Staff Representative

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 on:	October 2015
The implementation of this e-Safety policy will be monitored by the:	Dinas Powys Primary School e-Safety Group
Monitoring will take place:	Yearly and as required
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):	Yearly and as required
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:	July 2016
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	Vale of Glamorgan ICT Manager, Vale of Glamorgan Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) with support of the Vale of Glamorgan ICT Team
- Outcomes of meetings of the e-Safety Group