TAFF BARGOED
LEARNING PARTNERSHIP

'Learning and Growing Together'

Digital Safeguarding & E-Safety Policy

Policy Version: **1.2**

E-Safety Policy at Taff Bargoed Learning Partnership

Introduction

E-Safety is an issue that all staff within the Taff Bargoed Learning Partnership take seriously. 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. This policy has been written in accordance with the South West Grid for Learning guidelines, who are the professional body acknowledged for appropriate E-Safety.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Schoools within the Learning Partnership will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

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 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 (*it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor*).

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Officer
- regular monitoring of e-safety incident logs wihtin the school
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Head teacher and Senior Leaders:

The Head teacher 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 will be delegated to the *E-Safety Officer*. The Head teacher 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 – "Responding to incidents of misuse" and relevant *Merthyr Tydfil CBC* disciplinary procedures).

The Head teacher and Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Head teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Senior Management Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

Within the school, the day-to-day running of E-Safety remains the responsibility of the E-Safety Officer. The E-Safety Officer has a number of responsibilities as part of the role. This includes, but is not limited to;

- leading 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 training and advice for staff
- liaises with the Local Authority / relevant body when situations arise
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings including reporting to Governors
- reports regularly to Senior Leadership Team

The E-Safety officer will decide how incidents are to be dealt with, however the investigation / action / sanctions will be the responsibility of the Head teacher and Senior Leadership of the school. Depending on the severity of actions, some instances may also involve the school's designated Child Protection Officer.

Network Manager:

The school network is externally managed and maintained by the Local Authority. Although it is not the reposnsibilty of the school to directly manage the network, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-safety policy and procedures.

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The Local Authority's filtering policy, is applied and updated on a regular basis and that 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.
- that monitoring systems are implemented and updated as agreed in school policy

Teaching and Support Staff

There is a required level of responsibility required for teaching and support staff. Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or E-Safety Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems *e.g. Teachers2Parents, Office Email, Hwb*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer:

The Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection / 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Students / pupils:

Within the school, it is important that pupils develop their understanding that they are responsible for their actions. The responsibility for pupils, using the internet, include:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 / academy (where this is allowed)

<u>Community Users:</u>
We continue to find ways in which the Community can use our school and how we, as a school, can help to promote ICT amongst members of our community. 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.

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 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 Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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.

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 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

Education – The Wider Community

Where possible, our schools welcome opportunities for local community groups to use the school. Opportunities for the wider community to use ICT 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:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer will provide advice and training to individuals as required.

Training – Governors / Directors

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

- Attendance at training provided by the Local Authority / National Governors Association
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

Within the Taff Bargoed Learning Partnership, we have a managed ICT service provided by an outside contractor, therefore it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school Acceptable Use Agreements.

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 which includes;

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school academy 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 by the LA who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly. For pupils, group/class log-ons and passwords will be provided.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- Allyson Jones (ICT Technician) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided differentiated user-level filtering, allowing different filtering levels for different groups of users – staff / pupils)
- LA technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate 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.
- An agreed policy is in place regarding the use of removable media (eg memory sticks) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should never be published or 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, Twitter or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Permission for the use of photographs (through a general phtograph form) will be completed by parents during intake at school.
- 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 via an AUA signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement
- Pupil's work can only be published with the permission of the pupil and parents or carers.

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

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 should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is

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

Social Media – Protecting Professional Identity

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.

The school provides the following measures to ensure reasonable steps are in place to 12inimize risk of harm to pupils, staff and the school through limiting access to personal information:

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to 12inimize risk of loss of personal information. Settings on Social Media should prevent staff's images or information from being obtained.
- They do not make links or 'friends' with parents/carers of pupils within the school.

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

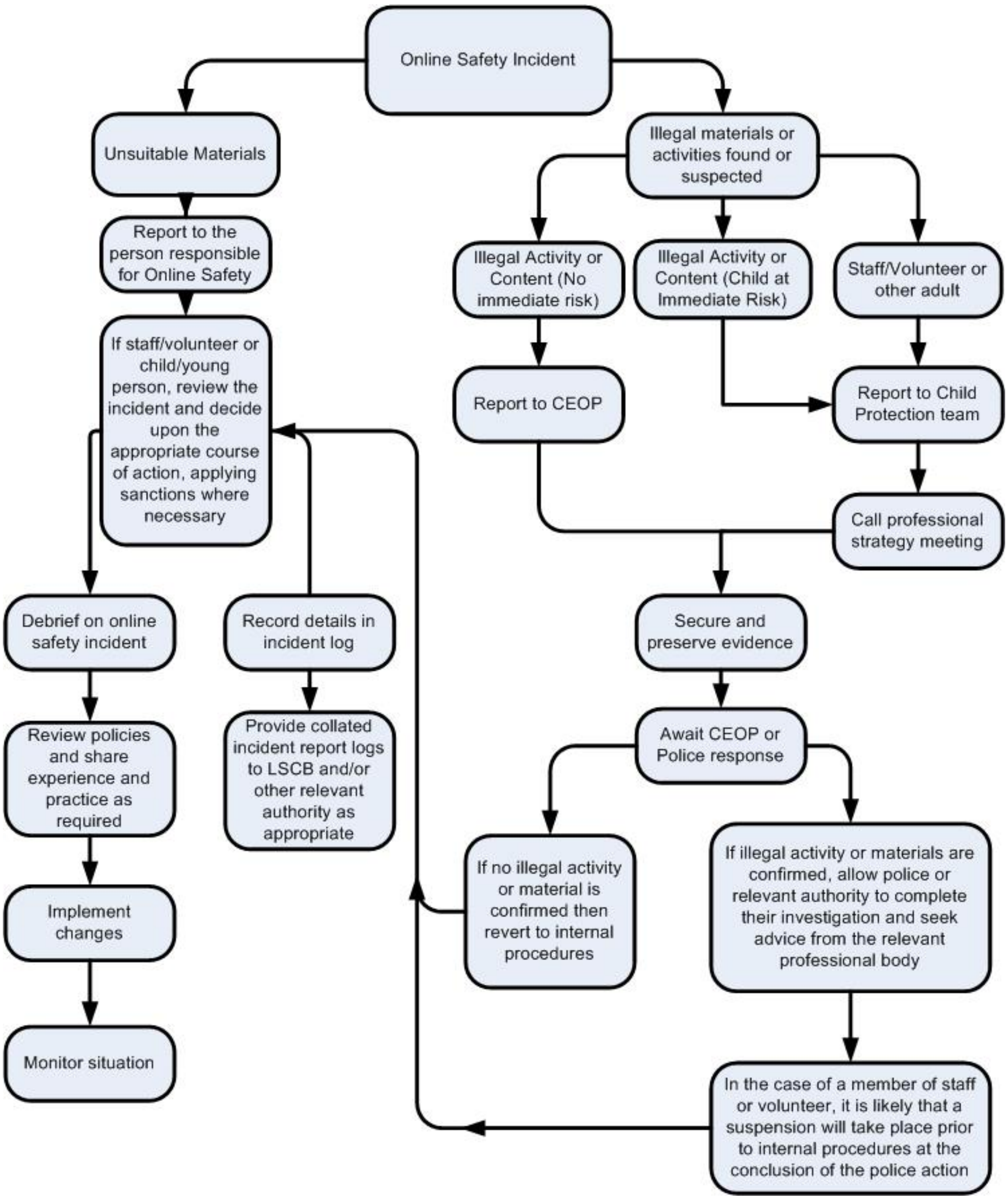
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				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			

llegal 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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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
  - 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

Pupils **Actions / Sanctions**

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							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X		X						
Unauthorised use of social media / messaging apps / personal email	X							X	
Unauthorised downloading or uploading of files	X								
Allowing others to access school network by sharing username and passwords	X		X				X		
Attempting to access or accessing the school network, using another pupil's account	X								
Attempting to access or accessing the school network, using the account of a member of staff	X		X				X		
Corrupting or destroying the data of other users	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			
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 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			X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X					X	

Staff **Actions / Sanctions**

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						
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	X			X		
Deliberate actions to breach data protection or network security rules		X	X			X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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 pupils		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			X		
Using proxy sites or other means to subvert the school's filtering system		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
Breaching copyright or licensing regulations	X	X	X					

Continued infringements of the above, following previous warnings or sanctions		X	X				X	X

Use of Mobile phones within our Schools

A key part of digital safeguarding within our schools, includes the use of mobile phones within our school settings. The Taff Bargoed Learning Partnership has a clear policy on the use of mobile phones within the school and this policy makes explicit reference to camera mobile phones.

Camera Mobile Phones

Camera mobile phones are now the norm and built in digital camera enables users to take high resolution pictures. These can be sent instantly to other mobile phone users or email addresses. They can also be posted on the internet or on social media sites. There is potential for camera mobile phones to be misused in schools, although this is rare amongst staff.

Staff & Agency Policy

Staff use of mobile phones during their working day must be:-

- **Outside of directed time/ contracted hours;**
- **Discreet and Appropriate i.e. not in the presence of pupils.**

Mobile phones should be switched off and **must be** left in a secure place (the school provides secure storage) which is **not** in the classroom, during lesson times. Mobile phones should not be present in classrooms, in order to protect and safeguard staff and pupils.

Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, they should use the school telephone in the office.

Staff should never sent, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.

This guidance should be seen as a safeguard for members of staff, the school and the Local Authority. Staff should understand that failure to comply with the policy is likely to result in the enforcement of the Whistleblowing policy and associated procedures.

Parents, Visitors or Volunteers in School Policy

Adults either in school or accompanying children on school trips should not use their cameras or mobile phone cameras to take pictures of pupils unless it is at a public event such as Sports Day or summer fete and are of their own children. Adults, visitors or volunteers in school should only use their mobile phone within the confines of the school office or staff room.

Pupil Policy

While we acknowledge the need for a pupil to bring a mobile phone to school if they walk to and from school without adult supervision. Outside of this, schools within the Taff Bargoed Learning Partnership do not allow pupils to bring mobile phones to school due to the potential issues raised above.

When a child needs to bring a phone into school, a permission slip (see Appendix 1) must be signed by the parents/guardian and the phone must be left with the class teacher at the start of the day and collected at the end of the day.

Phones should be clearly marked so that each pupil knows their own phone. Parents are advised that the School accepts no liability for the loss or damage to mobile phones which are brought into school or school grounds.

Where a pupil is found by a member of staff to be using a mobile phone, the phone will be confiscated from the pupil, handed to a member of staff in the school office who will record the name of the pupil and attach it to the phone. The mobile phone will be stored in the school office. The pupil may collect their phone at the end of the school day.

If a pupil is found taking photographs or video footage with a mobile phone of either pupils or staff, this will be regarded as a serious offence and action taken in line with our behaviour policy.

If images of other pupils or staff have been taken, the phone will not be returned to the pupil until the images have been removed by the people in the presence of a member of the SMT (Please see more guidance on sexting in our child protection policy).

Should a pupil be found using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able ot bring a phone into school.

We kindly ask parents/guardians, to talk to their children about the appropriate use of text messages as they can often be used to bully other pupils.

Should parents need to contact pupils or vice versa during the school day, this should be done via the usual school procedure of contacting the school office via phone or email.

Review

The policy supports the safeguarding policy. This policy will be monitored and reviewed as required but at least every two years.

Appendix 1

TAFF BARGOED
LEARNING PARTNERSHIP
'Learning and Growing Together'

MOBILE PHONE CONSENT

Dear Parent/Carer,

In accordance with our mobile phone policy, if your child is bringing in a mobile phone to school on a regular basis, please could you sign the form below to give your permission for your child to do this and remind them of our Policy.

- Your child needs to bring their phone to the school office first thing in the morning before they go their classroom.
- The school bears no responsibility for the loss or damage to a mobile phone
- Your child's phone should be appropriately marked so that they can recognise it
- Should your child be found using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring their phone into school.

Many thanks,

Mr R Morgan
Executive Head Teacher

TAFF BARGOED
LEARNING PARTNERSHIP
'Learning and Growing Together'

MOBILE PHONE PARENTAL CONSENT

I/we give permission for our child (name) ……………………………………………………
to bring their mobile phone into school.

We have read the policy and understand its implications.

Signed: ____________________________ Date: _________________

Please return permission slip to the school office. Thank you.