TAFF BARGOED LEARNING PARTNERSHIP

Parneriaeth Dysgu Taf Bargod

Online Safety Strategy

Introduction
"Children and young people need to be empowered to keep themselves safe. At a public swimming pool, we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." ***(Dr Tanya Byron, Safer Children in a Digital World (2008))*** As part of safeguarding and promoting the welfare of children and young people in accordance with the Children Act and Working Together to Safeguard Children, Taff Bargoed Learning Partnership have developed this online safety strategy built on four key areas: • Policies, practices, and procedures. • Education and training. • Infrastructure and technology. With more online traffic than ever before, learning how to stay safe and remain vigilant to the spread of disinformation has never been so important.

Purpose of the Strategy
As a partnership we are committed to raising awareness of online safety issues to all stakeholders within the organisation and promoting good practice to reduce risks to children and young people when they are online or when using digital electronic technologies. Our approach focuses on working with children and young people, their parents and carers, and the professionals who work with children and young people. Whilst we must understand the issues and risks posed, we must be careful not to demonise the technology and ensure that these are balanced with the immense opportunities and benefits that new technologies bring. Sexual communication with a child is an offence under the Serious Crime Act 2015 Circular 2017/01: Sexual communication with a child - implementation of s.67 of the Serious Crime Act 2015 - GOV.UK (www.gov.uk) This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years of age. It is an offence for an adult to arrange to meet with someone under 16 having communicated with them on just one occasion. Where there are concerns in relation to a child's exposure to extremist materials, the child's school may be able to provide advice and support: all schools are required to identify a Prevent Single Point of Contact (SPOC) who is the lead for safeguarding in relation to protecting individuals from radicalisation and involvement in terrorism.

Background

As a partnership, we agree that all agencies providing services to children have a duty to understand e-safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children.

In simple terms, online safety refers to the act of staying safe online. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets. Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardise their personal information, lead to unsafe communications or even affect their mental health and wellbeing.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our children and young people and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional, and educational contexts. However, alongside these benefits, there are potential risks that professionals have a statutory duty of care to manage, to ensure they do not become actual dangers to children. Social networking sites are often used by perpetrators as an easy way to access children and young people for sexual abuse. In addition radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity: this is similar to the grooming process and exploits the same vulnerabilities.

Online Safety Risks and Issues

Online safety risks and issues can be roughly classified into four areas: content, contact, conduct and contract.

The following are basic examples of the types of online safety risk and issues that could fall under each category:-

- engages with and/or is exposed to potentially harmful **CONTENT**.
- experiences and/or is targeted by potentially harmful **CONTACT**.
- witnesses, participates in and/or is a victim of potentially harmful **CONDUCT**.
- is party to and/or exploited by a potentially harmful **CONTRACT**.

CORE	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualisation of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalisation, and extremist recruitment	Potentially harmful user communities e.g self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design

Online Gaming
The above categories of risk and issues can be applied to online gaming, which we know many Pupils will take part in, alongside additional risks. • Content: All games carry an age restriction/certification. Children and young people should only have access to age related Computer Games. Some games are often violent and/or have some sexual element (Grand Theft Auto, Call of Duty, Resident Evil, etc) – these games do come with Certificate 18. • Contact: Risks can be posed when children access Online Gaming and chat rooms within the computer games themselves. • Content: Children and young people may act out certain scenarios from films or games that they have watched/played. They may follow an instruction/behaviour from what they have seen or by others they have met online whilst gaming. • Addiction/Overuse: For some young people gaming can become the most important aspect of their life it is important to provide and ensure that there is a balance of other activities. • Consumer: Games can require payment for skins (costumes), additional lives, access to additional levels. Need to ensure that links to adult's bank details are restricted. Parents and carers should be encouraged to talk to their children about what games or chat rooms they are playing/ have access to.

Harmful Challenges and Hoaxes
Online challenges often involve people recording themselves online doing something that is difficult or risky, which they share to encourage others to repeat it. Challenges can be dangerous and could result in substantial physical injury or permanent harm. Online hoaxes, sometimes known as pranks or scams, differ from challenges. A hoax is a deliberate lie designed to seem truthful. Some hoaxes can also include distressing self-harm or suicide narratives. The Department for Education (DfE), in collaboration with partners in the UK Council for Internet Safety Education subgroup and the Samaritans, has published advice for schools and colleges to support their approach to harmful online challenges and online hoaxes.

The Dark Web
The Child Exploitation and Online Protection Command (CEOP) of the National Crime Agency (NCA) has some resources for use by professionals and parents and carers to understand the dark web and to help them to have conversations with young people who may already be using the dark web. For more information please click here:- https://www.thinkuknow.co.uk/professionals/resources/dark-web-explained/

Online Safety - Whole School Approach

All school staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life.

Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

- CONTENT: It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

  Our Schools will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement. Online safety and the schools approach to it is outline in the child protection policy.

- FILTERS AND MONITORING: Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and LA staff do all that they reasonably can to limit children's exposure to the above risks from the school IT system.

How are children taught about online safety in school?

As part of mandatory RSE (Relationships and Sexuality Education) in primary and secondary schools, pupils are taught about online safety in an age-appropriate way. This includes being taught: • what positive, healthy and respectful online relationships look like
• the effects of their online actions on others
• how to recognise and display respectful behaviour online
• how to use technology safely, responsibly, respectfully and securely
• where to go for help and support when they have concerns

<u>In our schools, Pupils are also taught:</u>
• that people sometimes behave differently online, including by pretending to be someone they are not
• that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others
• the rules and principles for keeping safe online: how to recognise risks, harmful content and contact, and how to report them
• how to critically consider their online friendships and sources of information
• how information and data is shared and used online

KEY MEASURES FOR LIMITING ONLINE RISKS

The Taff Bargoed Learning Partnership support the use of the Becta PIES model which offers an effective strategic framework for approaching online safety. This model illustrates how a combination of effective policies and practices, education and training, infrastructure and technology underpinned by standards and inspection can be an effective approach to manage and limit online safety.

POLICIES AND PRACTICES

To support and ensure stakeholders develop and maintain robust and effective policies, practices and procedures to safeguard children and young people against online risks.

As a federation we will:-

- Appoint a dedicated online safety lead.
- Create and maintain an online safety policy.
- Make sure that appropriate Acceptable Use of ICT Policy and Staff User Agreements are in place.
- Have a procedure in place for reporting an e-safety incident, e.g., clear lines of reporting incidents of misuse of ICT by users and safeguarding incidents when a user is at risk or has come to actual harm using ICT.
- Review and evaluate all internal policies and procedures

INFRASTRUCTURE AND TECHNOLOGY

To identify and promote technologies, tools and infrastructure services which are carefully monitored, and which appropriately support online safeguarding priorities for children and young people and related stakeholders.

As a school who provide access to ICT, we will:

- identify all technologies used within the organisation itself and conduct risk assessments with regards to online safety -safety.
- Consider the use of additional software and/or settings for technologies to limit the e-safety risk.
- Use up to date security software / solutions for technologies.

• Where Internet access is available, ensure that a web content filtering product or service must as a minimum, ensure the following are blocked:
• Pornographic, adult, tasteless or offensive material.
• Violence (including weapons and bombs);
• Racist, extremist and hate material.
• Illegal drug taking and promotion.
• Criminal skills and software piracy.

EDUCATION AND TRAINING

To promote and support effective learning opportunities for all stakeholders which recognise and address current and emerging online safeguarding risks for children and young people.

As a school we aim to raise awareness of online safety through education and training. Online safety training is incorporated into our program of training e.g., safety awareness, acceptable use, safeguarding procedures.

This should include induction of new staff, plus on-going support, and supervision of existing staff. Staff will be made aware of local, regional, and national issues with regards to online safety and should be confident in their abilities to escalate an incident as necessary and appropriate.

It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will ask to access. There will be training resources and support materials dealing with the issues of online safety with children, young people, parents and professionals available within our schools.

Monitoring and Review

This strategy will be monitored and reviewed on an annual basis (or sooner in response to new technologies or online safety incidents).